Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

1995-03

An intrusion-detection tutoring system using means-ends analysis

Schiavo, Sandra Jean.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/35082

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL
Monterey, California

DTIC
ELECTE
MAY 2 4 1995
S D
G

THESIS

AN INTRUSION-DETECTION TUTORING SYSTEM USING MEANS-ENDS ANALYSIS

by

Sandra Jean Schiavo

March 1995

Thesis Advisor: Neil C. Rowe

Approved for public release; distribution is unlimited.

19950523 006

DTIC QUALITY INSPECTED 5

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time reviewing instructions, searching existing data sources gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 1995	Master's Thesis

4. TITLE AND SUBTITLE
An Intrusion-Detection Tutoring System Using Means-Ends Analysis

5. FUNDING NUMBERS

6. AUTHOR(S)
Schiavo, Sandra Jean

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/ MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/ MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the United States Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This research designed and implemented an intelligent tutoring system for teaching computer intrusion detection to potential or current system administrators of computer networks. The Intrusion-Detection Tutoring System (IDTS) is an intelligent tutoring system built using Quintus Prolog and METUTOR general-purpose tutoring software written by Professor Rowe. The operating environment of the IDTS is a virtual one, based on UNIX; it uses some common UNIX commands and file hierarchy. After both student and tutor analyze a static audit file to find suspicious and or malicious behavior, the student tries to fix the damage, and the computer critiques the student's actions using means-ends analysis. Using its nineteen behavior rules, IDTS can classify eleven different types of intruder behavior known to exploit system vulnerabilities, and can tutor the student how to detect this behavior and how to efficiently return the system to a secure state after the intrusion has occurred. Four different audit files of varying length were tested with IDTS. IDTS correctly identified most intruder behavior in both manually and computer generated audit files, and showed it could correctly tutor on that behavior.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Intrusion detection, intelligent tutor, means-ends analysis, computer security	156
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

AN INTRUSION-DETECTION TUTORING SYSTEM USING MEANS-ENDS ANALYSIS

Sandra Jean Schiavo
Lieutenant, United States Navy
B.S., Virginia Polytechnic Institute and State University, 1987

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL

March 1995

Accesion For
NTIS CRA&I ☒
DTIC TAB ☐
Unannounced ☐
Justification .....
By .....
Distribution /
Availability Codes
Dist | Avail and / or Special

Author: [redacted]
Sandra Jean Schiavo

Approved by: [redacted]
Neil C. Rowe, Advisor

[redacted]
Timothy J. Shimeall, Second Reader

[redacted]
Ted Lewis, Chairman,
Department of Computer Science

ABSTRACT

This research designed and implemented an intelligent tutoring system for teaching computer intrusion detection to potential or current system administrators of computer networks. The Intrusion-Detection Tutoring System (IDTS) is an intelligent tutoring system built using Quintus Prolog and METUTOR general-purpose tutoring software written by Professor Rowe. The operating environment of the IDTS is a virtual one, based on UNIX; it uses some common UNIX commands and file hierarchy. After both student and tutor analyze a static audit file to find suspicious and or malicious behavior, the student tries to fix the damage, and the computer critiques the student's actions using means-ends analysis. Using its nineteen behavior rules, IDTS can classify eleven different types of intruder behavior known to exploit system vulnerabilities, and can tutor the student how to detect this behavior and how to efficiently return the system to a secure state after the intrusion has occurred. Four different audit files of varying length were tested with IDTS. IDTS correctly identified most intruder behavior in both manually and computer generated audit files, and showed it could correctly tutor on that behavior.

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

Computer security of software and data is a difficult and never-ending problem requiring both manual and automated controls. A key part of the manual controls is the system administrator who is responsible for not only ensuring that the system is fully operational but also that it is secure. This person, in addition to learning day-to-day operation of the computer network, will have to learn about computer security either by reading about it or through trial by fire. This trial-by-fire method of learning about security can be potentially damaging to the company financially or to national security in the case of the military unit because security problems can be infrequent, although very damaging when they do occur. There has to be or should be a better way to learn about system administrator duties particularly security issues.

Formal computer security courses are available, but can be time consuming and cost prohibitive for some smaller organizations. What would be helpful is an automated intrusion-detection tutoring system that could teach the user about system security duties and how to identify an intruder from an audit trail. This type of intrusion-detection tutoring system would allow the user to learn about intruder behavior at their own convenience and pace, and possibly expedite the learning process. This thesis presents the Intrusion-Detection Tutorial System (IDTS), which is an automated intelligent tutoring system focussing on intrusion detection.

IDTS, described herein, is built using Quintus Prolog and runs on top of the metutor30 application, written by Professor Rowe, which uses intrusion-detection software and means-ends analysis to actually perform the tutoring. IDTS was specifically designed to tutor potential or current computer system administrators in the area of intrusion detection. The operating system environment of IDTS is a virtual one, based on UNIX; it uses some common UNIX commands and its file hierarchy. After both student and tutor analyze a static audit file to find suspicious and or malicious behavior, the student tries to fix the damage, and the computer critiques the student's actions using means-ends analysis.

The contents of this thesis are as follows. Chapter II will present related work in intelligent tutoring systems and means-ends analysis. Chapter III will discuss intrusion detection and automated systems to detect intruders, specifically the Next-Generation Intrusion Detection Expert System (NIDES) developed at SRI International, Menlo Park, CA. Chapter IV will introduce IDTS and take an in-depth look at its actual components. It will present the virtual computer operating environment of IDTS, specifically the file hierarchy, the audit file, the UNIX commands used, and the assumptions and decisions made during its design. It will also discuss the relationships between each of the components as well as additional required programs written by others. Chapter V will discuss the performance of the IDTS, specifically behaviors detected, space requirements, and CPU runtime. Chapter VI will summarize all of the above, and will discuss the weaknesses of the IDTS. It will also make recommendations for improving the existing IDTS application. Finally, two appendices have been included. Appendix A contains the source code for IDTS, and Appendix B contains script runs of IDTS, testing four separate input audit files.

II. INTRODUCTION TO MEANS-ENDS ANALYSIS AND INTELLIGENT TUTORING SYSTEMS

A. MEANS-ENDS ANALYSIS

Means-ends analysis attempts to solve a a search problem through abstraction by taking the difference between the current state and the goal state and applying a recommended operator. In order to apply a recommended operator, some preconditions must be met. The results of applying an operator are postconditions, which are added to the state. It is also possible that by applying an operator, conditions may be deleted from the state. Means-ends analysis is a recursive search; therefore, it will continue to apply operators, check preconditions, add postconditions, and delete postconditions, until the difference between the state and the goal is the empty set. In an implementation of means-ends analysis, the recommended operators are stored as **recommended** facts, the preconditions as **precondition** facts, the postconditions as **addpostcondition** facts, and the deleted postconditions as **deletepostcondition** facts [Ref. 1]. For an in-depth explanation of means-ends analysis, see [Ref. 1, pp. 263 - 281].

B. INTELLIGENT TUTORING SYSTEMS

Intelligent tutoring systems offer an attractive and efficient way to learn, since the emphasis is on learning-by-doing: converting factual knowledge into experiential knowledge [Ref. 2, p. 1]. They provide an interactive simulation for the student to learn procedural skills, and a friendly environment in which the student can back-up and redo actions. There are also similar intelligent tutoring systems that provide a shell for "role-performance" skills that are the same as procedural skills [Ref. 3]. Both "role-performance" and procedural skills are type of skills the student learns by completing a series of discrete actions. An example of a procedural skills intelligent tutoring system is PIXIE, described in [Ref. 4]. It is an expert system shell for teaching rule-based systems. It has features for knowledge representation and for defining inference rules in the domain. There are also tutoring strategy rules present in PIXIE. Regardless of the implementation,

all intelligent tutoring systems will require a large predefined task structures library used to store the components of the tutoring strategies to be designed by the teacher or expert.

IDTS uses the intelligent tutoring system METUTOR to tutor the student in intrusion detection. METUTOR, like PIXIE, is a procedural skills tutoring system and uses mean-ends analysis to tutor the student using the recommended operator predicates described above. A procedural intelligent-tutoring system, like METUTOR, is suited to intrusion detection because the task of finding intruders and correcting the damage they cause is procedural in nature.

III. AN INTRODUCTION TO INTRUSION DETECTION

Today it is not uncommon to pick up a newspaper or magazine and read that someone has broken into the computer system of a major company or university. The reasons why someone breaks into a computer system are numerous. Some do it just for the mere thrill of it, while others do it to cause problems within the computer system like inserting a virus. More and more intruders, however, are doing it for monetary gain. "Cybercrime" is on the rise, and current laws do not apply well at all to computer crimes [Ref. 5].

According to Lunt in [Ref. 6],"timely detection of unauthorized intruders into computers and computer networks is a problem of increasing concern." Regardless of the reason for computer intrusion, detecting this intruder behavior, whether it is an external penetration or an insider attack, should be of the utmost importance to any system administrator. There are several software intrusion-detection tools available to a system administrator as well as hardware tools; both types of tools require analysis of audit trail information as stated in [Ref. 7].

A. INTRUSION-DETECTION SOFTWARE TOOLS

1. Expert Systems

In an intrusion-detection expert system, there are a set of rules based on the "expert's" knowledge of the intruder's behavior used to analyze the contents of the audit trail. If behavior exists in the audit trail matching the any of the rules, then some alarm is triggered. In addition to these rules based on past intrusions, known as system vulnerabilities, there are also rules corresponding to anomalous behavior. User profiles are maintained on legitimate users on the system, and if there is any deviation from their established pattern, due to an intruder using the account, then it is considered an anomalous detection [Ref. 9]. A well-known intrusion-detection expert systems is described in the following section.

2. Next-Generation Intrusion Detection Expert System (NIDES)

NIDES is a real-time intrusion-detection expert system developed at SRI International, Menlo Park, CA, and it provides a good example of a class of similar systems. Its predecessor, Intrusion-Detection Expert System (IDES), has been the basis for most intrusion detection research to date, and it forms the conceptual basis for several other intrusion-detection software tools [Ref. 7]. NIDES is system independent, and is able to process the audit trail information from a target system. It uses expert-system rules, modeled for different types of intruder behavior, to detect intruders regardless if they are external penetrators, internal penetrators, or misfeasors. When intruder behavior is detected based on these rules, an alarm is raised. For the masquerader intruders, NIDES maintains statistical profiles of past user behavior. If the user's activities vary from the established behavior pattern, referred to as an anomalous detection, then NIDES also sounds an alarm [Ref. 6].

B. PROBLEMS IN INTRUSION DETECTION

1. Audit Trail Overhead and Reduction

Since IDTS is based on UNIX, we will discuss its auditing facilities. Depending on the version of UNIX used, either Berkeley or System V, all will maintain log files. These log files form the basis of UNIX's auditing system. A determined system administrator may find unauthorized and or suspicious behavior by reviewing these log files. All versions of UNIX maintain the following log files [Ref. 8, p. 125]:

- **•usr/adm/lastlog** Logs each user's most recent login time
- **•etc/utmp** Logs a record each time a user logs in.
- **•/usr/adm/wtmp** Logs a record each time a user logs in or logs out.
- **•/usr/adm/acct** Logs every command run by every user.

Depending on the number of users, the information gathered in these four files can be an enormous amount of information for a system administrator to wade through. In [Ref. 6], Lunt says that the far too much information is collected to be useful to determine if intruders are present, and that information that could be used in find intruders is not

collected. Reducing the amount of audit trail information and deciding which information to keep is an on-going research problem in intrusion detection.

2. Behavior Classification

A big problem with automated intrusion-detection systems is that they may incorrectly classify user behavior. There are "false negatives" when an intruder is classified as a legitimate user, and "false positives" when a user is mistakenly called an intruder.

3. Intrusion Detection Training

Although automated intrusion-detection systems, like NIDES, make a system administrator's life easier, it is still up to them to make the final call whether suspicious behavior in an audit file belongs to an intruder. This is especially true in NIDES, since when a user's profile is first being trained there are several false positive alerts. In these cases, the system administrator must intervene and reset the intrusion-detection system. This is one of the reasons NIDES was not used. Regardless if an automated intrusion-detection tool is used, the system administrator must be knowledgable in intrusion detection and know what to do if an intrusion has occurred. Cleaning-up after an intruder attack is something an automated system will not teach a system administrator.

The rules in most intrusion-detection systems, like in NIDES, are modeled for real-time detection, and do not teach any basic system administrator skills such as storing backup tapes once they are done using them. What is needed is a tutor to teach an administrator not only how to detect intruder behavior, but what to do after an intruder has penetrated their system and about basic system administrator duties. IDTS is capable of both teaching the student how to detect intruder behavior and how to fix the damage caused by the intruder. Also with IDTS, there are rules that focus on basic system administrator skills which are well-documented in system administrator books and reports. IDTS is described in the following chapter.

IV. THE INTRUSION-DETECTION TUTORING SYSTEM (IDTS)

IDTS is an intelligent tutoring system written in Quintus Prolog. It runs on top of the metutor30 application, written by Professor Rowe, which provides means-end analysis of student actions and general-purpose rules for tutoring. It can be run in any operating system environment which has a Quintus Prolog compiler installed.

A. OPERATION OF IDTS

Upon executing IDTS, the user is shown an audit file and the mail messages received by root for a virtual computer system. It is up to the user to choose which actions to perform based on the audit file contents. The tutoring system will know the best recommended way to approach the intruder behavior present in the audit trail and prevent it from occurring again. If the user chooses an inappropriate action, the tutor will notify the user that a more appropriate action exists. If the chosen action is appropriate, but there is a more important action to perform, the tutor will give a hint to the user. The tutor will only end the lesson when the user has corrected any and all security problems present in the audit file, although the user can quit before completing the tutorial. The details of how IDTS accomplishes the tutoring and its components will be explained later in this chapter; however, before the actual components of IDTS can be understood, the virtual environment in which it operates must be explained.

B. THE VIRTUAL ENVIRONMENT OF IDTS

The virtual computer environment modeled for this tutoring system is based on the UNIX operating system. It was chosen due to its known security flaws and its widespread use, especially in the academic community. Although commands found in the audit trail are UNIX commands, several liberties and assumptions about them were made to accommodate the tutoring system. The goal of this tutor is not to make the user an expert on UNIX, but to make them aware of the types of behaviors that hard-core hackers and even

casual hackers use to disrupt, corrupt, or abuse time on a given system. Some familiarity with UNIX, however, would be beneficial to the user, but is not required.

1. File Hierarchy

The files used in IDTS are virtual files, that is, they do not exist. By a virtual file what is meant is the file has a name, size, directory in which it resides, time it was last modified, permissions, type, and owner, but there is no actual content to the file.

a. System Files

As in any UNIX system, we have virtual system files like in a typical UNIX environment. These system files are owned by the system administrator who will be called **root**. For simplicity sake, only a few of the major system files that are known to most users have been used.

b. User Files

It is important that our virtual world include the most tempting system files like "passwd" and those files located in the "bin" directory belonging to root, but user files are also present for a more realistic environment. The files are stored just as they would be in a UNIX environment. Each user has a subdirectory under root's directory named "users." Each user can then create and own as many files and subdirectories as they desire. Figure 1 shows an example of what a file directory tree in this modeled environment might look like.

c. Operations on Files

Like the files themselves, operations on the files are virtual. If the audit file were to show that a user edited a file, the only parts of the file description which would change would be the file's size and last time modified. When a file is created or deleted, a

new file description is created and placed in the database or the file information is removed from the database respectively.

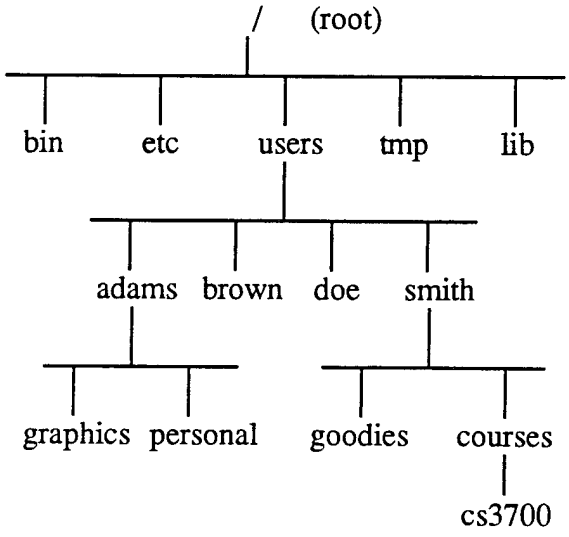

Figure 1: Example of Directory Tree

2. Audit File

The pseudo-UNIX operating system audit trail in the virtual computer system of IDTS is not as sophisticated as a true UNIX operating system. There are only five pieces of information stored in each record of the audit file: user name, time, current directory, UNIX command issued, and the result of issuing the particular UNIX command. Figure 2 is an example listing of the audit file.

This file is a simplified consolidation of the four log files included a UNIX computer system. To assist the user, extra information not available in a true UNIX system is also in the audit file: the arguments of commands issued and the directory in which they were issued [Ref. 8, p. 130]. Additionally, the result of the command executed is given: if the command is unsuccessfully executed, this is "fail;" if a file is created or modified, this is the size of the resulting file in bytes; if a mail message is sent, this is the message itself; otherwise, this is "ok."

Name	Time	Path	Command	Result
brown	1030	none	login brown	fail
brown	1031	none	login brown	fail
brown	1032	none	login brown	fail
brown	1033	none	mail root	bad(password,brown)
doe	8982	none	login doe	ok
doe	9315	doe	emacs bigpaper	29947
doe	9335	doe	emacs csproject	1024
doe	9352	doe	ls	ok
doe	9360	doe	emacs csproject	4096
doe	9373	doe	mail root	bad(ls,bin)
doe	9375	doe	mail root	bad(doefile,doe)
doe	9379	doe	logout	ok
jones	910	jones	su	fail
jones	910	none	login jones	ok
jones	911	jones	su	fail
jones	912	jones	su	fail
jones	920	jones	su	ok
jones	921	root	cd ~farmer	ok
smith	859	none	login smith	ok
smith	900	smith	cd etc	ok
smith	901	etc	cp passwd ~smith	ok
smith	902	etc	logout	ok

Figure 2: Example Audit File Listing

a. Concept of Time

Time (t) is represented as an increasing integer value starting at the value one (t=1).

3. UNIX Commands Recognized by IDTS

a. Logins

The login command as it appears in an IDTS audit file can be seen in Figure 2 as "login <username>." For simplicity, it is assumed that a user can login legitimately only once in the IDTS virtual UNIX environment. This restriction assists with determining if a user's password has been compromised when a user is logged in twice and there is no logout between the two login times.

b. Su Command

The ***su*** or super-user command allows a user to shut down the system, terminate any process, create new accounts, change any account's password, or read, write, or delete any file on the entire system regardless of its permissions [Ref. 10, p. 35]. An intruder will either try to login directly as the super-user root, or simply attempt to execute the su command from within another user account. If an intruder is successful at becoming the super-user, the consequences could be grave.

In IDTS it is assumed that root is the only user who should know the root password to execute the su command successfully; therefore, if the su command is successfully executed by a user other than root, then the root password has been compromised. This assumption is an unreasonable restriction for root in a true UNIX operating environment, since the user who is root would not be able to execute this command in any directory other than their own. But this restriction teaches the user that an intruder will try everything in their power to become root.

c. File Commands

There are three types of file commands modeled in IDTS: copying, editing/ creating, and deleting files. In the audit file the command used for copying a file is the UNIX *cp* command which takes two arguments, the file being copied and the location to which it will be copied. The editing/creating a file command is the UNIX ***emacs*** command which takes one argument, the file to be edited or created. The command used to delete a file is the UNIX ***rm*** command which takes one argument, the file to be deleted.

Two assumptions have been made in the area of file manipulation for IDTS: a user must be located in the same directory of the file they wish to manipulate, and the only editor available in IDTS's virtual UNIX operating environment is *emacs*.

C. PROGRAM OVERVIEW

IDTS code consists of one main program and eight primary submodules. Appendix A contains the source code for these modules. Three of the eight submodules for this tutor

were written by Professor Rowe. These three modules are *metutor30*, *megraph30*, and *filetree*. The last two modules provide an XWindows graphical user interface.

1. The Tutoring System Design

The tutor program requires six modules: *intruder*, *metutor30*, *rules*, *operators*, *files*, and a test *auditfile*. Figure 3 shows the relationship between all IDTS modules.

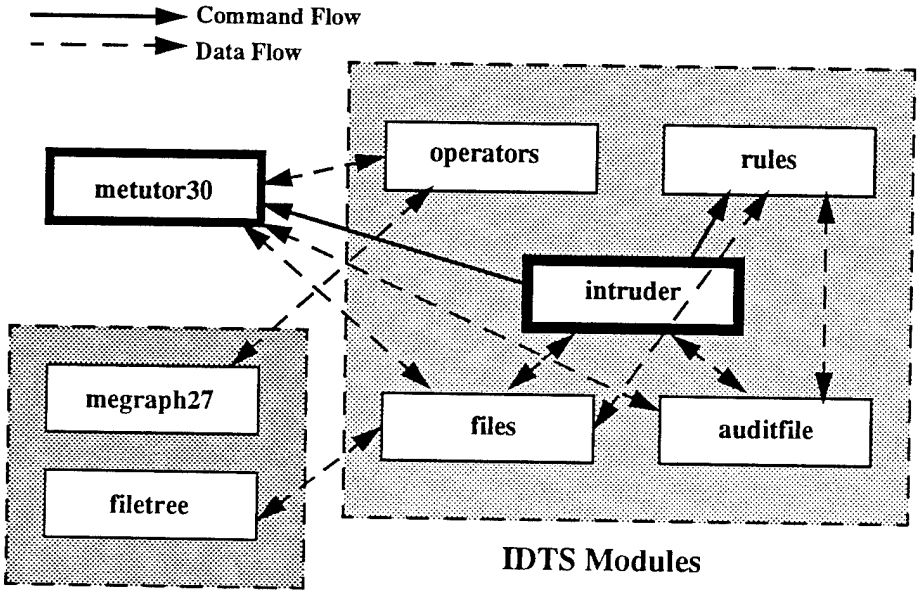

Figure 3: Relationships Between IDTS Modules

The *intruder* module is the main program, and it initializes the system and passes the start_state and goal of the tutoring system to the *metutor30* module which determines how to tutor the user. The *rules* module contains all of the rules used to detect intruder behavior based upon the *auditfile* contents. The *operators* module holds all possible student operators/actions in the form of Prolog facts for **recommended**, **precondition**, **addpostcondition**, and **deletepostcondition** conditions. These four predicates are used by the *metutor30* module to tutor the student.

The *auditfile* contains **audit** facts that are either generated by the threat modeling program developed by LT Christopher Roberts described in [Ref. 11], or are manually

written. To avoid unnecessary problems for the student, this file is a static file, unlike the real world where the audit trail is dynamic. Otherwise, for example, right at the moment the user has selected an action to get rid of a certain behavior, another audit trail fact could add another behavior to the state which needs to be removed. The *files* file is comprised of **file** facts which contain the initial virtual file hierarchy and **insecure_password** facts which tell the tutor the users who have insecure passwords. The **file** facts are dynamic, and may be created, modified, or deleted based on the actions in the *auditfile*.

D. DATA STRUCTURES

1. File Facts

a. System Files

The data structure for files in the virtual computer system are in the form of a seven argument predicate called **file**. The following is an example of the **file** predicate:

file(<filename>,<directory>,<owner>,<size>,<type>,<protection>,<time>),

where

<filename> is any acceptable UNIX filename;

<directory> is any acceptable UNIX directory;

<owner> is the name of a user on the system and owner of this file;

<size> is an integer and the size of the file in bytes;

< type> is the type of the file, either executable or text;

<protection> are the acceptable UNIX permissions for the file;

and <time> is the time the file was last modified by the <owner>.

The seven arguments are the typical information one might see as a result of using the **ls** command in a UNIX environment or **dir** in a DOS environment.

b. Derived Files

There are three different types of derived file facts: **deleted_dir**, **deleted_file**, and **modified_file** facts. They are derived by means of the *checkfiles*

subroutine in the *intruder* module which loops through all of the audit file facts and applies any deletions of files and or directories and any modifications to the existing system files. Their arguments are the same as those of the regular system **file** facts.

2. Audit File Facts

a. Audit Facts

The only data structure stored in the *auditfile* is the **audit** fact. The form of these facts is as follows:

audit(<user>,<time>,<directory>,<command>, <result>).

where

<user> is the name of a user in the system;

<time> is the time the <user> executed the particular <command>;

<directory> is the name of the current directory the <user> is located in;

<command> is any acceptable UNIX command;

and <result> is the result of executing the particular <command>, either "ok," "fail," "bad(<filename>,<directory>)," or an integer indicating the new size of the file named in the <command>.

b. Behavior Facts

The four and five argument **behavior** facts are derived from the audit facts by applying the behavior rules in the *rules* module. The four argument **behavior** facts are of the form:

behavior(<intruder>,<crime>,<start>,<end>).

where

<intruder> is a string and the name of the user in the system suspected of the <crime>;

<crime> is a string representing the type of suspicious or malicious behavior the <intruder> is accused of;

<start> is an integer and the time the <crime> became noticeable;

<end> is an integer and the time that the <crime> ended.

The five argument **behavior** fact is the same as the four argument **behavior** fact except that it has an extra argument called <object>. The form of the five argument behavior facts is as follows:

behavior(<intruder>,<crime>,<object>,<start>,<end>).

The <object> argument is a string and the name of an object, either a file's name or user's password, that has been altered by the <crime> the <intruder> is suspected of.

c. Mail Facts

Like the four and five argument **behavior** facts, **mail** facts are also derived from the auditfile **audit** facts. The **mail** fact contains a complaint from a user to root about a file in a directory or a password of a given user. The complaint may be that a file has been modified, deleted, or that something strange occurs when the given file is executed. If the complaint concerns a user's password, it means that the password has been changed by another person, possibly an intruder. An assumption is made that a user can send a mail to root even though their password has been changed. The **mail** facts are initially stored in the following data structure in the audit file in the <result> argument of the **audit** fact:

bad(<filename>,<directory>).or **bad**(password,<user>).

where

<filename> is the name of a file in the system;

<directory> is the name of the directory in which this particular file resides;

and <user> is the name of a user on the system. This data structure is changed by the *checkfiles* routine into another form and is stored in the database as:

mail(<from>,<to>,<time>,<message>).

where

<from> is the name of the user who sent the <message>;

<to> is the name of the user who receives the <message>;

<time> is the time the <message was sent by <from>;

and <message> is the mail message in the same form as the **bad** predicate.

3. Miscellaneous Facts

a. Insecure_Password Facts

The **insecure_password** fact is a simple data structure which is part of the initial files IDTS uses to initialize the system. They let the tutoring system know which users have insecure passwords. These facts are contained in the *files* module. Their data structure is as follows:

insecure_password(<user>).

where <user> is the name of any user in the system.

E. IDTS MAIN MODULE -- INTRUDER

1. Initializing the Start State

In order to run IDTS, the start_state of the tutor must be initialized. This is accomplished by the subroutine *checkfiles* in the *intruder* module. The *checkfiles* subroutine is called by the main outer loop *start* of the tutor. *Start* not only calls *checkfiles*, but is also displays the *auditfile* and mail received by root, asserts a graphicsflag, and calls the main loop *go* of the *metutor30* module.

a. Checkfiles

The *checkfiles* subroutine systematically loops through the *auditfile* "looking" at every **audit** fact. Figure 4 shows how this is done. Depending on the command in the **audit** fact, either nothing is done or one of the seven subroutines in *checkfiles* is executed. These seven subroutines will now be described.

The *rm_star* subroutine deletes all files in a given directory by asserting a **deleted_file** fact in the database for each **file** fact in the directory where the "rm *"command is issued. To simulate the action of actually deleting a file, *rm_star* then retracts each **file** fact in the given directory. By first asserting the **deleted_file** fact in the database, the original seven arguments of the **file** fact are preserved. Preserving these arguments is necessary if a deleted file is to be restored from backup.

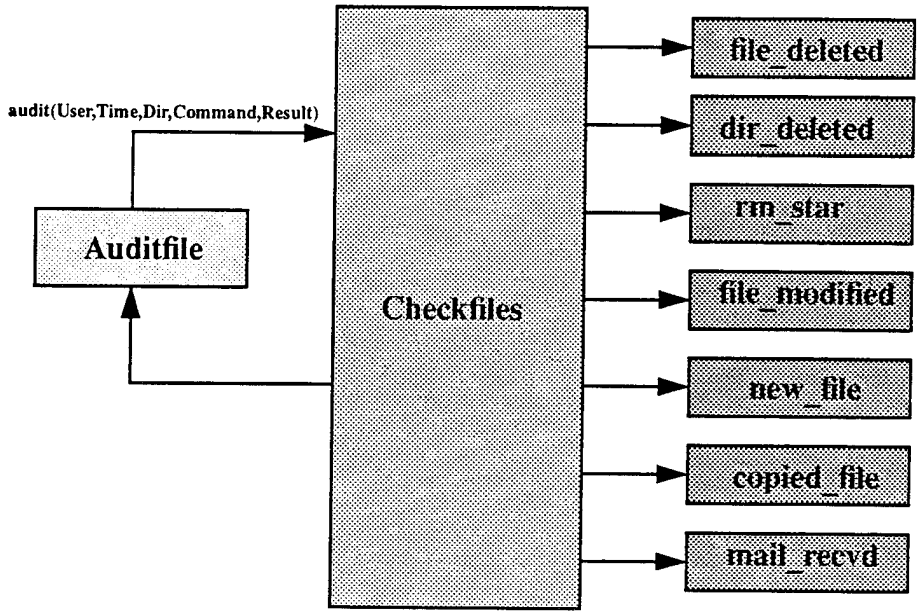

Figure 4: Checkfiles Routine

The *file_deleted* subroutine handles a command argument in an **audit** fact of the form "rm Filename," where Filename is any existing file. Like *rm_star*, *file_deleted* asserts a **deleted_file** fact, and then simulates deleting the file by retracting the **file** fact. In *dir_deleted* a **deleted_dir** fact is asserted vice a **deleted_file** fact.

If an **audit** fact has the command argument "emacs Filename" then the subroutine *file_modified* asserts a **modified_file** fact in the database for "Filename," thus preserving the original state of the file in case it needs to be restored from backup later. The original **file** fact is then retracted and a new **file** fact with the modified size and time is asserted. If the same file is modified more than one time in the audit file, the second time it is modified, that is the command "emacs Filename" is issued more than once, the subroutine *file_modified* will fail. The reason for this failure, is only one modified_file fact should be asserted into the database, since there can only be one set of file arguments to use

to restore from backup. It should be noted that the current state of the file will always reflect the most recent modifications.

The *new_file* subroutine handles the case when a file is created, or if an **audit** fact has a command argument of the form "emacs Filename," where Filename is any non-existing file. A new **file** fact is asserted into the database. Five of the seven **file** fact arguments are taken directly from the **audit** fact: Filename, Directory, User, Size, and Time. The Type and Protection arguments of the new file fact are given the default values of "text" and "-rw-r--r--" respectively.

The *copied_file* subroutine creates a new file in the given path with the same size, type, protection, and time last modified as the original. The filename, directory, and owner may vary. The file may be copied to another directory in the same account as the file being copied, or it may be copied to another account; the subroutines *same_account* and *different_account* handle these situations respectively. A new **file** fact is asserted in the database.

Finally, the subroutine *mail_recvd* manages mail messages to root. This command causes *mail_recvd* to assert a **mail** fact into the database.

b. Forming Start State List

When the *checkfiles* subroutine is done, the initial start_state list can be formed by collecting facts into small lists by the utilities **nice_bagof** and **nice_setof**, written by Professor Rowe, and appending them together.

In addition to the facts asserted during the execution of the *checkfiles* subroutine, **file**, **behavior** and **insecure_password** facts as well as the fact that the backup tape is stored, are appended to the start_state list. The **file** facts are those after the *checkfiles* subroutine has been executed; therefore, any files created, deleted or modified as a result of this subroutine's execution will be reflected. The **behavior** facts are determined by the behavior rules for suspicious and blatant malicious behavior in the rules module. The

specifics of how these **behavior** facts are determined will be discussed in detail later. The **insecure_password** facts are given in the *files* file.

2. Initializing the Goal State

The goal of the Intrusion Detection Tutoring System is for the user to identify any suspicious and or malicious behavior based on a review of the audit file and mail received by root and to correct any of this observed behavior. Additionally, the user should ensure that there are no insecure passwords, the system backup tape is stored properly, and the password cracker has been executed at least once.

The goal of the tutor as stated above has to be put into a form the tutor can use. Like the start_state, the goal is in the form of a list. The first and main part of the goal is to not have any **behavior** facts true; therefore, the goal contains a list of **behavior** facts preceded by the word "**not.**" This is accomplished by taking advantage of the subroutines *suspicious_behavior* and *not_item*. *Suspicious_behavior* yields a list of **behavior** facts; *not_item* takes this list and returns a list of **not(behavior)** facts. Similarly, to obtain the goal of no insecure passwords, a list of **insecure_password** facts is run through the *not_item* subroutine yielding a list of **not(insecure_password)** facts. The second part of the goal is easily satisfied by appending:

[**stored**(backup,tape),**executed**(password,cracker)].

3. Output

There are two main output subroutines used in the main outer loop start of the tutor, *auditfile* and *mail*. The *auditfile* subroutine sorts the contents of the audit file alphabetically and chronologically, and outputs it at the beginning of the tutoring session. The *mail* subroutine sorts the messages received by root alphabetically and prints them to the screen. Both *auditfile* and *mail* use the subroutine *fixed_length_concatenate* from the module *filetree* to assist in output formatting.

F. RULES MODULE

1. Behavior Rules

The rules module uses four and five-argument behavior rules to determine suspicious and or malicious behavior based on the audit file facts in a chronologically sorted audit file. There are nineteen behavior rules that detect eleven different types of intruder behavior. The behavior rules are only invoked at the tutor's initialization. They address three types of intruders:

1. someone who has guessed the root password
2. someone who has guessed another user's password
3. someone who is a malicious insider

An intruder is recognized by one of five ways: 1) they successfully executed the *su* command and they are not root; 2) they guessed another user's password, and there is evidence of a concurrent login or they changed the user's password; 3) they copied and or edited the system password file "passwd" successfully; 4) they successfully copied and or edited a file belonging to another user in the other user's account; and 5) they successfully edited a system executable file located in the "bin" directory.

They find evidence for the following types of intruder behavior:

•an intruder maliciously deleted a file

(Root receives a message from a user that one of their files has been deleted, and there is evidence in the audit file that someone else has deleted it. By "maliciously" deleted what is meant is that an intruder has deleted, in this case, a file that does not belong to him. He was able to delete it by either by becoming super-user or by simply going to the directory where the file resides and deleting it. In the general sense, anytime an object, either a user's file or password, is changed or deleted by a user who does not own it, it is considered "malicious" behavior.)

•an intruder copied the system password file

(There is evidence in the audit file that the password file has been copied by some user.)

•an intruder edited the system password file
(There is evidence in the audit file that the password file has been edited by some user.)

•an intruder maliciously changed user password
(Root receives a message from a user that their password has been changed.)

•an intruder inserted a Trojan Horse
(Root receives a mail message that a system executable file is bad, and there is evidence in the audit file that it has been modified by some user by a given amount. In IDTS, a Trojan Horse is defined as 1024 bytes change in an executable file.)

•an intruder maliciously modified file
(Root receives a message from a user that one of their files has been modified.)

•a compromised root password exists
(A user other than root has successfully executed the *su* command or there is a concurrent login of root.)

•a compromised user password exists
(There is a concurrent login of a user.)

•a possible Trojan Horse exists
(Root receives a mail message that a system executable file is bad, and there is evidence in the audit file that it has been modified by some user.)

•a possible intruder exists
(There is evidence in the audit file that a user is repeatedly trying to execute the su command.)

•a possible compromised user password exists.
(There is evidence in the audit file of a suspicious login by a user.)

Two important subroutines used by the behavior rules are *concurrent_login* and *suspicious*. The subroutine *concurrent_login* is used by the behavior rules to determine if a user is logged on twice. It compares a user's login and logout times to see if there is a case when there are two login times where no logout time exists between them. The *suspicious* subroutine is used to determine when a legitimate user or intruder has

repeatedly failed executing a particular command. There are three suspicious commands that the behavior rules look at: logins and the use of the *su* command. If the command fails more than some pre-determined threshold, then it is considered suspicious behavior.

G. OPERATORS MODULE

This module stores the predicates required by metutor30 to tutor the student: **recommended**, **precondition**, **addpostcondition**, and **deletepostcondition**. The possible student actions and their recommending circumstances are stored in the **recommended** predicate. In order to use one of these recommended actions, the student and tutor must ensure that certain preconditions are met. A list of preconditions for each operator action is in the **precondition** predicate. After an operator action has been selected by the student and executed by the tutor, any postconditions associated with the operator action are placed in the current state of the system. These postconditions are stored in the **addpostcondition** predicate. The **deletepostcondition** predicate is used to delete a fact from the current state after the associated operator has been applied to the current state of the system. In IDTS, the most important actions are those which remove the intruder behaviors from the states, and move the student closer to the goal.

The recommended operators in IDTS were developed from reviewing system administrator responsibilities in intrusion detection in [Ref. 8]. The following is a list of IDTS operators available to the student:

- restore the system password file "passwd" from backup
- change the permissions on the "passwd" file
- change the root password
- remove a Trojan Horse from a file
- compare a file for a Trojan Horse with its backup version
- confront a user
- restore a user's password
- issue a new user password
- examine a user's password
- investigate a user's password

•restore the modified file X from backup
•restore the deleted file X from backup.
•check the permissions on a file
•execute the password cracker
•change the password for a user
•find the file X on the backup tape
•locate the backup tape
•load the backup tape
•store the backup tape.

A student uses these operators to reach the goal of no intruder behavior in the state. For example, if an intruder had maliciously deleted a file belonging to another user, the tutor would recommend the "restore the deleted file X from backup." operator to remove the behavior fact "**behavior**(Intruder,'maliciously deleted file',X,Time1,Time2)" from the current state. In order to apply the "restore" operator, the precondition "found the file X on the backup tape" must be satisfied which means the student needs to apply the "find the file X on the backup tape" operator; however, this also has a precondition of "loaded the backup tape," and so on. Figure 5 shows all the steps to remove the fact "**behavior**(Intruder,'maliciously deleted file',X,Time1,Time2)" from the state.

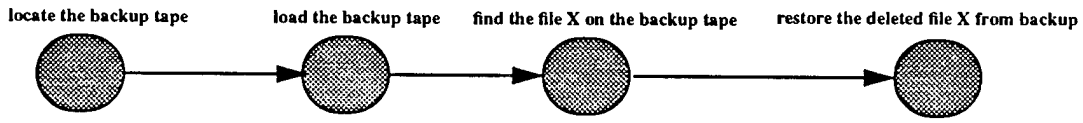

Figure 5: Example of Using Operators to Remove Intruder Behavior

By applying the appropriate operators, the student will ultimately reach the point where all intruder behavior has been addressed and system administrator responsibilities are completed, like storing the backup tape if it was loaded to restore a file from backup.

At this point, the tutor will exit with congratulating the student on successfully finishing the lesson.

V. DISCUSSION OF RESULTS

A. IDTS PERFORMANCE

Four runs of IDTS were conducted with different sized test audit files containing a variety of intruder behaviors. The first run used an input audit file written by the author. The other runs used input audit files generated by the threat modeling program written by LT Christopher Roberts described in [Ref. 11]. The input audit files used and scripts of each run are contained in Appendix B. A discussion of the results of these runs follow.

1. Run 1

The first run of IDTS used a one hundred and seven **audit** fact test audit file. All eleven different types of intruder behavior modeled in IDTS described in Chapter IV were present in the test audit and were detected. These eleven types of behaviors were found in twenty **behavior** facts determined by the IDTS rules. The memory required for this run totalled 4,188,640 bytes, and had a runtime of 81.7 seconds.

2. Run 2

The second run of IDTS used a test audit file consisting of one hundred and ninety-five **audit** facts. Upon execution of IDTS, ten **behavior** facts were found, correctly detecting six different types of intruder behavior. There was a user, "doe," who successfully added an executable file to root's "bin" directory. IDTS does not model this type of intruder behavior; however, it is something to consider for IDTS's future. Also, removing any copies of the system password file "passwd" could be modeled in future versions of IDTS. The memory required for this run totalled 2,353,632 bytes, and had a runtime of 40.5 seconds.

3. Run 3

The largest audit used contained two hundred and nineteen **audit** fact test audit file, and was generated with similar parameters as the audit in run 2. IDTS correctly identified seven different types of intruder behavior from the behavior rules firing and finding

fourteen **behavior** facts. Again, the system password file was copied, but the copies remained in the directories to where they were copied. The memory required for this run totalled 2,484,704 bytes, and had a runtime of 40.3 seconds.

4. Run 4

The fourth run of IDTS was performed on a two hundred and ten **audit** facts input file, and was generated with similar parameters as the audit in run 2. Ten **behavior** facts were found by the IDTS rules, correctly identifying five different types of intruder behavior. The memory required for this run totalled 2,222,560 bytes, and had a runtime of 26.9 seconds.

5. IDTS Tutoring Performance

The goal of the tutor is to have the student remove any intruder behavior found by the IDTS rules, execute the password cracker, remove any insecure user passwords that result from executing the password cracker, and ensure the backup tape is stored. For example, in run 1 all eleven types of intruder behavior were present in the input audit file. The tutor will expect the student to select the appropriate actions to remove these behaviors. In this run, the student starts by selecting the operator "execute the password cracker." It finds that there are only two passwords known to be insecure. Again the tutor will expect the student to remove these behaviors. By applying the appropriate action, "change the password," for each user with an insecure password, the student accomplishes this. The student in run 1 systematically removes all behaviors by restoring files, examining and changing passwords, confronting users, as well as completing the required system administrator actions, like properly handling the backup tape. After all behaviors and insecure passwords are removed, the password cracker is executed, and the backup tape is stored, the tutor congratulates the student for having done the job.

In all runs, the tutor correctly tutored the student, and the student was able to remove all behaviors detected by the IDTS rules and complete all required system administrator duties like executing the password cracker.

B. HARDWARE AND SOFTWARE REQUIREMENTS

The source code for IDTS requires 38,561 bytes. Including an average-sized input audit file (100 **audit** facts) and the initial system files file, this size increase to approximately 49,500 bytes. Since it is written in Quintus Prolog, a Prolog compiler is necessary to run this application, which increases the space requirements. IDTS can run without the graphical user interface provided by the programs *megraph30* and *filetree* to reduce space requirements of the windowing environment of XWindows.

VI. CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

Intrusion detection is a very big problem, and will more than likely be a problem in the future. There are too many variables involved with determining if a system has come under an attack by an intruder. Although there are automated intrusion detection systems available, they do not always detect intruder behavior and are susceptible to false negatives and false positives. The final burden to find the intruder ultimately falls upon the system administrator. The system administrator should then understand how to analyze audit trail information. The IDTS is a tool which can assist the system administrator in learning how to analyze an audit trail and detect an intruder based on this analysis.

A. PROGRAM CONTRIBUTIONS

To date, IDTS is the first intelligent tutoring system focused on intrusion detection. It has nineteen behavior rules that capably and correctly detect eleven different types of intruder behavior, as demonstrated by the test runs in Appendix B. IDTS is flexible and has the ability to tutor a student in different scenarios by means of using multiple audit files.

B. PROGRAM WEAKNESSES

The behavior rules that are part of IDTS have been tested on only a few sample audit files, and require a more thorough testing. They detect behavior that has been written to match them. For example, the rules did not detect the user "doe" from run 2 who planted an executable file (possible virus) in the "bin" directory. This is definitely a rule which should be included in future versions of IDTS. IDTS also does not have any statistical anomaly detection capability. This is a difficult obstacle for IDTS to overcome, since it concerns itself exclusively with logical reasoning and it is built on a virtual environment. Anomaly detection could perhaps be simulated, but requires considerable overhead required to maintain and train profiles. Finally, IDTS is not system independent; the rules are written for UNIX systems.

C. FUTURE RESEARCH DIRECTIONS FOR IDTS

The best way to improve IDTS would be to make it a more generic intrusion-detection tutoring system. This would mean it would have to be system independent. A possible solution would be to incorporate NIDES detection rules into IDTS to find the intruders. Then the other parts of IDTS along with the *metutor30* module would tutor the student based on the intruder behavior detected by NIDES. Also, by using NIDES the problem of IDTS lacking anomalous detection capability would be solved.

Additionally, more rules and operators should be added to make IDTS more comprehensive. Rules to detect numerous file "permission denied" errors and numerous "cd" command executions could be modeled. Also, rules as well as operators dealing with intruders who penetrate systems via modem or **rlogins** could and should be incorporated in IDTS. More operators on networking and system administrator responsibilities should be added too. For example, operators like terminating network connections and closing firewalls when an intruder is suspected could be added. As for system administrator responsibilities, operators such as removing copies of the system password file, checking for dormant accounts, killing processes, disabling accounts, and informing the authorities can only enhance IDTS and make the student a well-rounded system administrator.

LIST OF REFERENCES

1. Rowe, N. C., *Artificial Intelligence Through Prolog*, Prentice-Hall, Inc., 1988.

2. Sleeman, D., Brown, J. S., *Intelligent Tutoring Systems*, Academic Press Inc. (London) Ltd., 1982.

3. Guralnik, D., Kass, A., "An Authoring System for Creating Computer-Based Role-Performance Trainers," World Conference on Educational Multimedia and Hypermedia, Vancouver, Canada, June 1994, pp. 235-240.

4. Sleeman, D., "PIXIE: A Shell for Developing Intelligent Tutoring Systems," *Artificial Intelligence in Education*, Volume 1, pp. 239-265, Ablex, Norwood, NJ, 1987.

5. Meyer, M., "Stop! Cyberthief!," *Newsweek*, February 6,1995, pp. 36-38.

6. Lunt, T. F., "Detecting Intruders in Computer Systems," *1993 Conference on Auditing and Computer Technology*, Computer Science Laboratory, SRI International, Menlo Park, CA, 1993.

7. Marshall, V. H., "Intrusion Detection in Computers," *Summary of the Trusted Information Systems (TIS #348) Report on Intrusion Detection Systems*, January 1991.

8. Garfinkel, S., Spafford, G., *Practical UNIX Security*, O'Reilly & Associates, Inc.,1991.

9. Frank, J., *Artificial Intelligence and Intrusion Detection: Current and Future Directions*, University of California at Davis, June 9, 1994.

10. Curry, D. A., *UNIX System Security: A Guide for Users and System Administrators*, Addison-Wesley Publishing Company, Inc., 1992.

11. Roberts, C. C., *Plan-Based Simulation of Malicious Intruders on a Computer System*, Master's Thesis, U.S. Naval Postgraduate School, Monterey, CA, March 1995.

APPENDIX A: IDTS SOURCE MODULES

This appendix contains the source code for IDTS.

Tab 1. IDTS Main Module -- Intruder
Tab 2 IDTS Rules Module
Tab 3. IDTS Operators Module
Tab 4. IDTS Files Module
Tab 5. IDTS Sample Auditfile Module

TAB 1. IDTS MAIN MODULE -- INTRUDER

```
/*****************************************************************************/
/* Intrusion-Detection Tutoring System Program (IDTS)                        */
/* LT Sandra J. Schiavo, U.S. Navy, Naval Postgraduate School, Monterey CA 93940 */
/*****************************************************************************/
/* IDTS Main Interface -- Version 1                                          */
/*                                                                           */
/*    To run IDTS, load *this* module and query:                             */
/*                                                                           */
/*         :-  start.                                                        */
/*                                                                           */
/*    NOTE:  To run IDTS with an XWindows graphical user interface query:    */
/*                                                                           */
/*         :-  winstart.                                                     */
/*                                                                           */
/*    The main interface module initializes IDTS by passing and passes the start */
/* state and goal to the metutor30 module.                                   */
/*****************************************************************************/

:-ensure_loaded(metutor30),asserta(writelist_prednum(1)),
  ensure_loaded(auditfile),
  ensure_loaded(filetree),
  ensure_loaded(rules),
  ensure_loaded(files),
  ensure_loaded(operators).

/*****************************************************************************/
/*  The singular predicate is used to help with verb tense of the output     */
/*****************************************************************************/

singular(behavior(A,B,C,D)).
singular(behavior(A,B,C,D,E)).
singular(adams).
singular(evans).
singular(jones).
singular(davis).

/*****************************************************************************/
/*  These predicates are hidden from the user.  They are used by the tutor.  */
/*                                                                           */
/*    behavior/4                                                             */
/*    behavior/5                                                             */
/*    file/7                                                                 */
/*    deleted_dir/7                                                          */
/*    deleted_file/7                                                         */
/*    modified_file/7                                                        */
/*    insecure_password/1                                                    */
/*                                                                           */
/*****************************************************************************/

hidden(behavior(A,B,C,D)).
hidden(behavior(A,B,C,D,E)).
hidden(file(Name,Owner,Parent,Type,Size,Protection,Modified)).
hidden(deleted_dir(Name,Owner,Parent,Type,Size,Protection,Modified)).
hidden(deleted_file(Name,Owner,Parent,Type,Size,Protection,Modified)).
hidden(modified_file(Name,Owner,Parent,Type,Size,Protection,Modified)).
hidden(insecure_password(User)).

/*****************************************************************************/
```

```
/*  Usercommand allows for its argument to be used an appropriate action for the */
/*  student.                                                                      */
/*******************************************************************************/

usercommand(auditfile).
usercommand(mail).


intro('
************************************************************************
*                                                                      *
*  To see a list of possible actions, type the letter "h" or the word  *
*  "help." To review the audit file or your mail at anytime, type the  *
*  word "auditfile" or "mail" respectively.                            *
*                                                                      *
************************************************************************').

winstart:- asserta(graphicsflag),auditfile,checkfiles,mail,go.
start:-    auditfile,checkfiles,mail,go.


/*******************************************************************************/
/* The start state and goal passed to the metutor30 module to tutor student.   */
/*******************************************************************************/

start_state(Start):-
   nice_bagof(file(A,B,C,D,E,F,G),file(A,B,C,D,E,F,G),Files),
   mail_received(Mail),
   append(Files,Mail,L1),
   files_deleted(F1),
   append(L1,F1,L2),
   dirs_deleted(Dirs),
   append(L2,Dirs,L3),
   rm_files_deleted(RF1),
   append(L3,RF1,L4),
   files_modified(F2),
   append(L4,F2,L5),
   suspicious_behavior(Behavior),
   append(L5,Behavior,L6),
   insecure(Passwords),
   append(L6,Passwords,L7),
   append(L7,[stored(backup,tape)],Start),file_display_init(Start).

goal(Goal):- suspicious_behavior(Behavior),
   insecure(Passwords),
   not_item(Behavior,NotList1),
   not_item(Passwords,NotList2),
   append(NotList1,NotList2,NotList),
   append(NotList,[stored(backup,tape),executed(password,cracker)],Goal).


/*******************************************************************************/
/*  IDTS initializing routine:  checkfiles                                     */
/*******************************************************************************/

checkfiles:- not(checkedfiles).
checkedfiles:-
   audit(User,Time,Path,Command,Result),
   (file_deleted(Command,F1);
   dir_deleted(Command,Dir);
   rm_star(Command,Path);
```

```
    file_modified(Time,Path,Command,Result,F2);
    new_file(User,Time,Path,Command,Result);
    copied_file(User,Time,Path,Command,Result);
    mail_recvd(User,Time,Command,Result)),fail.

/*****************************************************************************/
/*  Checkfiles subroutines                                                   */
/*****************************************************************************/

files_deleted(Files):-
   nice_setof(deleted_file(F,Parent,Owner,Type,Size,Protection,Modified),
      deleted_file(F,Parent,Owner,Type,Size,Protection,Modified),Files).

file_deleted(Command,File):-
   make_list(Command,[rm,File]),
   file(File,Parent,Owner,Type,Size,Protection,Modified),
   (Type=text;Type=executable),
   asserta(deleted_file(File,Parent,Owner,Type,Size,Protection,Modified)),
   retract(file(File,Parent,Owner,Type,Size,Protection,Modified)).

dirs_deleted(Dirs):-
   nice_setof(deleted_dir(Dir,Parent,Owner,Type,Size,Protection,Modified),
      deleted_dir(Dir,Parent,Owner,Type,Size,Protection,Modified),Dirs).
dir_deleted(Command,Dir):-
   make_list(Command,[rmdir,Dir]),
   file(Dir,Parent,Owner,Type,Size,Protection,Modified),
   Type=directory,
   asserta(deleted_dir(Dir,Parent,Owner,Type,Size,Protection,Modified)),
   retract(file(Dir,Parent,Owner,Type,Size,Protection,Modified)).

rm_files_deleted(Files):-
   nice_setof(deleted_file(F,Parent,Owner,Type,Size,Protection,Modified),
      deleted_file(F,Parent,Owner,Type,Size,Protection,Modified),Files).

rm_star(Command,Path):-
   make_list(Command,[rm,*]),
   file(File,Path,Owner,Type,Size,Protection,Modified),
   (Type=text;Type=executable),
   asserta(deleted_file(File,Path,Owner,Type,Size,Protection,Modified)),
   retract(file(File,Path,Owner,Type,Size,Protection,Modified)).

files_modified(Files):-
  nice_setof(modified_file(File,Parent,Owner,Type,Size,Protection,Modified),
     modified_file(File,Parent,Owner,Type,Size,Protection,Modified),Files).
file_modified(Time,Parent,Command,Result,File):-
   make_list(Command,[emacs,File]),
   file(File,Parent,Owner,Type,Size,Protection,Modified),
   (Type=text;Type=executable),
   not(modified_file(File,Parent,Owner,_,_,_,_)),
   asserta(modified_file(File,Parent,Owner,Type,Size,Protection,Modified)),
   retract(file(File,Parent,Owner,Type,Size,Protection,Modified)),
   asserta(file(File,Parent,Owner,Type,Result,Protection,Time)).

file_modified(Time,Parent,Command,Result,File):-
   make_list(Command,[emacs,File]),
   file(File,Parent,Owner,Type,Size,Protection,Modified),
   (Type=text;Type=executable),
   retract(file(File,Parent,Owner,Type,Size,Protection,Modified)),
   asserta(file(File,Parent,Owner,Type,Result,Protection,Time)).
```

```
new_file(User,Time,Parent,Command,Result):-
   make_list(Command,[emacs,File]),
   not(file(File,Parent,_,_,_,_,_)),not(Parent=bin),
   asserta(file(File,Parent,User,text,Result,'-rw-r--r--',Time)).

new_file(User,Time,Parent,Command,Result):-
   make_list(Command,[emacs,File]),
   not(file(File,Parent,_,_,_,_,_)),(Parent=bin),
   asserta(file(File,Parent,User,executable,Result,'-rw-r--r--',Time)).

copied_file(User,Time,Parent,Command,Result):-
   make_list(Command,[cp,File,Path]),
   (different_account(User,Time,Parent,Command,Result,File,Path);
   same_account(User,Time,Parent,Command,Result,File,Path)).

different_account(User,Time,Parent,Command,Result,File,Path):-
   make_path_list(Path,[X|List]),
   tilde_word(X,Owner),
   file(File,Parent,_,Type,Size,Protection,Modified),
   (Type=text;Type=executable),
   not(file(File,Owner,Owner,_,_,_,_)),
   asserta(file(File,Owner,Owner,Type,Size,Protection,Modified)).

same_account(User,Time,Parent,Command,Result,File,Path):-
   make_path_list(Path,List),
   last(List,NewFile),next_to_last(List,Dir),
   file(File,Parent,User,Type,Size,Protection,Modified),
   (Type=text;Type=executable),
   not(file(File,Dir,User,_,_,_,_)),
   asserta(file(File,Dir,User,Type,Size,Protection,Modified)).

mail_recvd(User,Time,Command,Result):-
   make_list(Command,[mail,root]),
   asserta(mail(User,root,Time,Result)).

suspicious_behavior(Behavior):-
   nice_setof(behavior(User,Crime,Time1,Time2),
      Crime^Time1^Time2^behavior(User,Crime,Time1,Time2),B1),
   nice_setof(behavior(User,Crime,File,Time1,Time2),
      Crime^File^Time1^Time2^behavior(User,Crime,File,Time1,Time2),B2),
   append(B1,B2,B3),
   remove_behavior(B3,Behavior).

remove_behavior(List,Answer):-
   member(behavior(User,Crime,T1,T2),List),
   member(behavior(User1,Crime,T5,T6),List),
   (not(User=User1);not(T1=T5);not(T2=T6)),!,
   delete(behavior(User1,Crime,T5,T6),List,NewList),
   remove_behavior(NewList,Answer).

remove_behavior(List,Answer):-
   member(behavior(User,Crime,Object,T1,T2),List),
   member(behavior(User1,Crime,Object,T5,T6),List),
   (not(User=User1);not(T1=T5);not(T2=T6)),!,
   delete(behavior(User1,Crime,Object,T5,T6),List,NewList),
   remove_behavior(NewList,Answer).

remove_behavior(List,List).

insecure(Passwords):-
   bagof(insecure_password(User),insecure_password(User),Passwords).
```

```
mail_received(Mail):-
   nice_setof(mail(User,root,Time,Result),
   Time^Result^mail(User,root,Time,Result),Mail).

/*****************************************************************************/
/* Utility routines                                                          */
/*****************************************************************************/

not_item(List,NotList):-  not_item1(List,[],NotList).
not_item1([],List,List).
not_item1([A|List],ItemList,Answer):- F=..[not,A],
   not_item1(List,[F|ItemList],Answer).

next_to_last(List,X):-
   append(_,[X,Y],List),!.


/*****************************************************************************/
/*  Output routines:  auditfile and mail                                     */
/*****************************************************************************/

auditfile:-
   write('
*******************************************************************************
*                                                                             *
*                                AUDIT FILE                                   *
*                                                                             *
*      The following displays the current contents of the audit file:         *
*                                                                             *
*******************************************************************************
'),nl,

write('
Name       Time     Path           Command       Result'),nl,nl,
   view_audit,nl.
view_audit:- not(reviewed_audit).
reviewed_audit:-
   bagof(audit(User,Time,Path,Command,Result),
      audit(User,Time,Path,Command,Result),List),
   sort(List,Sorted),member(audit(User,Time,Path,Command,Result),Sorted),
   fixed_length_concatenate(User,Time,15,String1),
   write(String1),write('     '),
   fixed_length_concatenate(Path,Command,25,String2),
   write(String2),write('     '),
   write(Result),nl,fail.

mail:-
   write('
*******************************************************************************
*                                                                             *
*                                MAIL RECEIVED                                *
*                                                                             *
*      The following displays mail received by root:                          *
*                                                                             *
*******************************************************************************
'),nl,

write('
From        To      Time       Problem(File,Directory)'),
   nl,nl,read_mail,nl.
```

```
read_mail:- not(read).
read:-
   bagof(mail(User,root,Time,Problem),
      mail(User,root,Time,Problem),List),
   sort(List,Sorted),member(mail(User,root,Time,Problem),Sorted),
   mail(User,root,Time,Problem),
   fixed_length_concatenate(User,'root',15,String1),
   write(String1),write('     '),
   fixed_length_concatenate(Time,'',6,String2),
   write(String2),write('     '),
   write(Problem),nl,fail.
```

TAB 2. IDTS RULES MODULE

```
/*****************************************************************************/
/* Intrusion-Detection Tutoring System (IDTS)                                */
/* LT Sandra J. Schiavo, U.S. Navy, Naval Postgraduate School, Monterey CA 93940 */
/*****************************************************************************/
/* IDTS Rules Module                                                         */
/*                                                                           */
/*    This module contains the behavior rules which detect suspicious and    */
/* mailicious behavior present in the auditfile, and the various subroutines */
/* used in them.                                                             */
/*****************************************************************************/


/*****************************************************************************/
/*                              Behavior Rules                               */
/*****************************************************************************/

behavior(Intruder,'maliciously deleted file',File, T1, T1) :-
   audit(Intruder,P1,Time1,C1,ok),
   make_list(C1,[cd,X]),
   tilde_word(X,User),
   audit(Intruder,T1,Dir,C2,ok),
   make_list(C2,[rm,File]),
   not(audit(User,Time,Dir,C2,ok)),
   deleted_file(File,Dir,Owner,Type,Size,Protection,Modified).


behavior(Intruder,'maliciously deleted file',File, T1, T1) :-
   audit(Intruder,_,Time1,C1,ok),
   make_list(C1,[cd,X]),
   tilde_word(X,User),
   audit(Intruder,T1,Dir,C2,ok),
   make_list(C2,[rm,*]),
   not(audit(User,Time,Dir,C2,ok)),
   deleted_file(File,Dir,Owner,Type,Size,Protection,Modified).


/*****************************************************************************/
/*   System Administrator receives mail from a User saying a File was        */
/*   maliciously deleted by someone else.Case where malicious user cd's      */
/*   over to person's account.                                               */
/*****************************************************************************/

behavior(Intruder,'maliciously deleted file',File, T1, T2) :-
   audit(User,T2,P,'mail root',Message),
   Message=..[bad,File,Dir],
   audit(Intruder,P1,Time1,C1,ok),
   make_list(C1,[cd,X]),
   tilde_word(X,User),
   audit(Intruder,T1,Dir,C2,ok),
   make_list(C2,[rm,File]),
   not(audit(User,Time,Path,C2,ok)).


/*****************************************************************************/
/*   System Administrator receives mail from User saying Files were          */
/*   maliciously deleted by someone else.Case where malicious user cd's      */
/*   over to person's account and uses "rm *" to delete all files in a       */
/*   directory (Dir).                                                        */
```

```
/********** ***************************************************************************/

behavior(Intruder,'maliciously deleted file',File, T1, T2) :-
   audit(User,T2,_,'mail root',Message),
   Message=..[bad,_,Dir],
   audit(Intruder,_,Time1,C1,ok),
   make_list(C1,[cd,X]),
   tilde_word(X,User),
   audit(Intruder,T1,Dir,C2,ok),
   make_list(C2,[rm,*]),
   not(audit(User,Time,Dir,C2,ok)),
   T1<T2,
   deleted_file(File,Dir,Owner,Type,Size,Protection,Modified).


/*****************************************************************************************/
/* System Administrator examines audit file and sees that the password file      */
/*   has been copied or edited by some user(Intruder).                           */
/*****************************************************************************************/

behavior(Intruder,'copied password file', T1, T1) :-
   audit(User,T1,etc,Command,ok),
   make_list(Command,[cp,passwd,X]),
   make_path_list(X,[Y|List]),
   tilde_word(Y,Intruder).

behavior(Intruder,'copied password file', T1, T1) :-
   audit(Intruder,T1,etc,Command,ok),
   make_list(Command,[cp,passwd|List]).

behavior(Intruder,'edited password file', T1, T1) :-
   audit(Intruder,T1,etc,Command,Number),
   make_list(Command,[emacs,passwd]).


/*****************************************************************************************/
/* System Administrator examines audit file and sees a suspicious login and     */
/*   possible compromise of some user(User)'s password.                          */
/*****************************************************************************************/

behavior(User,'possible compromised user password',User,T1, T2) :-
   suspicious(login,User,Time,T1),
   audit(User,T2,Path,Command,ok),
   make_list(Command,[login,User]),
   time_difference(T1,T2).


/*****************************************************************************************/
/* System Administrator examines audit file and sees two users logged on at      */
/*   the same time with the same user name.                                      */
/*****************************************************************************************/

behavior(User,'compromised user password',User,T1, T2) :-
   concurrent_login(User,T1,T2).


/*****************************************************************************************/
/* System Administrator receives mail from user(X) saying that he cannot        */
/* login due to his password being changed.                                      */
/*                                                                               */
/* Case 1:  Intruder becomes root and changes user password.                     */
```

```
/* Case 2:  Intruder masquerades as user and changes password.                */
/*****************************************************************************/

/* Case 1 */

behavior(Intruder,'maliciously changed user password',User,T1, T2) :-
   audit(User,T2,Path,'mail root',Message),
   Message=..[bad,password,User],
   not(audit(User,_,_,yppasswd,ok)),
   audit(Intruder,_,_,C1,ok),
   make_list(C1,[cd,X]),
   tilde_word(X,User),
   audit(Intruder,T1,User,yppasswd,ok).

/* Case 2 */

behavior(User,'maliciously changed user password',User,T1, T2) :-
   audit(User,T2,P,'mail root',Message),
   Message=..[bad,password,User],
   audit(User,Time,Path1,Command,ok),
   make_list(Command,[login,User]),
   Time<T2,
   audit(User,T1,Path2,yppasswd,ok),
   T1>Time,T1<T2.


/*****************************************************************************/
/* Intruder has cracked the root password. Assumes only one person can       */
/* be root and must login as root.                                           */
/*****************************************************************************/

behavior(Intruder,'compromised root password', T1, T1) :-
   audit(Intruder,T1,Path,su,ok),
   not(Intruder = root).

behavior(root,'compromised root password', T1, T2) :-
   concurrent_login(root,T1,T2).


/*****************************************************************************/
/* System Administrator receives mail from user(X) saying that strange       */
/* "things" happen when he runs an executeable. Case when a system executable*/
/* has been modified.                                                        */
/*****************************************************************************/

behavior(Intruder,'possible Trojan Horse', File,T1, T1) :-
   audit(Intruder,T1,bin,C2,Size),
   make_list(C2,[emacs,File]),
   modified_file(File,bin,root,executable,_,_,_).


/*****************************************************************************/
/* System Administrator examines audit file and finds that user(X) has       */
/* successfully modified an executeable File by X amount. X in this case is  */
/* 1024.                                                                     */
/*****************************************************************************/

behavior(Intruder,'inserted Trojan Horse',File, T1, T2) :-
   audit(_,T2,Path,'mail root',Message),
   Message=..[bad,File,Dir],
   audit(Intruder,T1,Dir,C2,Size),
```

```
    make_list(C2,[emacs,File]),
    T1<T2,
    change_in_file(File,1024).


change_in_file(File,Size):-
    file(File,Dir,root,executable,Size2,Protection,Modified2),
    modified_file(File,Dir,root,executable,Size1,Protection,Modified1),
    Change is Size2 - Size1, Change = Size.


/*****************************************************************************/
/* System Administrator receives mail from user(X) saying that some of       */
/* his files have been maliciously modified. Case when malicious user        */
/* gains access to user(X)'s account by insecure password.                   */
/*****************************************************************************/

behavior(User,'maliciously modified file',File,T1, T2) :-
    audit(User,T2,P,'mail root',Message),
    Message=..[bad,File,Dir],
    suspicious(login,User,Time1,Time2),
    audit(User,T1,Dir,C2,Size),
    make_list(C2,[emacs,File]),
    T1<T2.


/*****************************************************************************/
/* System Administrator receives mail from user(X) saying that some of       */
/* his files have been maliciously modified. Case where malicious user(Y)    */
/* cd's to user(X)'s directory and modifies file directly.                   */
/*****************************************************************************/

behavior(Intruder,'maliciously modified file',File,T1, T2) :-
    audit(User,T2,P,'mail root',Message),
    Message=..[bad,File,Dir],
    audit(Intruder,Time1,P1,C1,ok),
    make_list(C1,[cd,X]),
    tilde_word(X,User),
    audit(Intruder,T1,Dir,C2,Size),
    make_list(C2,[emacs,File]),
    T1<T2,Time1<T2.

behavior(Intruder,'maliciously modified file',File,T1, T2) :-
    audit(User,T2,P,'mail root',Message),
    Message=..[bad,File,Dir],
    audit(Intruder,Time1,P1,C1,ok),
    make_list(C1,[cd,Dir]),
    audit(Intruder,T1,Dir,C2,Size),
    make_list(C2,[emacs,File]),
    T1<T2.


/*****************************************************************************/
/* Possible intruder on system due to multiple failed "su" commands.         */
/*****************************************************************************/

behavior(User,'possible intruder',T1, T2) :-
    suspicious('use of su command',User,T1,T2).

/*****************************************************************************/
/* Suspicious predicates                                                     */
```

```
/*****************************************************************************/

suspicious(login,User,T1,T2) :-
   repeated_failure(User,Command,Number,Times),
   make_list(Command,[login,User]),
   (Number >= 3),
   close_times(Times,[X|List]),
   get_times(X,T1,T2).

suspicious('use of su command',User,T1,T2) :-
   repeated_failure(User,su,Number,Times),
   not(User=root),
   (Number >= 3),
   get_times(Times,T1,T2).


repeated_failure(User,Command,Number,Failures1) :-
   bagof(Time,Path^audit(User,Time,Path,Command,fail),Failures),
      length(Failures,Number),sort(Failures,Failures1).


/*****************************************************************************/
/*                 Time Related Subroutines                                  */
/*****************************************************************************/

concurrent_login(User,Time1,Time2) :-
   logins(User,Logins),
   logouts(User,Logouts),
   concurrency(Logins,Logouts,Time1,Time2).

logins(User,Logins):-
   nice_bagof(Time,check(login,User,Time),L),
   sort(L,Logins).
logouts(User,Logouts):-
   nice_bagof(Time,check(logout,User,Time),L),
   sort(L,Logouts).

check(login,User,Time):- audit(User,Time,Path,Command,ok),
   make_list(Command,[login,User]).


check(logout,User,Time):- audit(User,Time,Path,Command,ok),
   make_list(Command,[logout]).


concurrency([X,Y],[],Y,100000).
concurrency([X],List,X,100000):- fail,!.
concurrency([X,Y|List1],[Z|List2],Y,Z):- Z > Y.
concurrency([X,Y|List1],[Z|List2],Y,Z):-
   append([Y],List1,NewList),
   concurrency(NewList,List2,Y,Z).
concurrency([],[],Number,100000):- fail,!.

close_times([X,Y,Z|List],Ans):- compare_times([X,Y,Z]),
   close_times1(List,Y,Z,[[X,Y,Z]],Ans).
close_times([X,Y,Z|List],Ans):- close_times1(List,Y,Z,[],Ans).
close_times1([],Y,Z,List,List).
close_times1([Z|List],X,Y,Newlist,Ans):- compare_times([X,Y,Z]),
   close_times1(List,Y,Z,[[X,Y,Z]|Newlist],Ans).
close_times1([Z|List],X,Y,Newlist,Ans):-
   close_times1(List,Y,Z,Newlist,Ans).
```

```
compare_times([T1,T2,T3]):- T2-T1<3,T3-T2<3.

time_difference(T1,T2):- (T1 - T2)< 5.

get_logout(User,Logout):-
   not(audit(User,Time,Path,logout,ok)),
   Logout is 100000.

get_logout(User,Logout):-
   audit(User,Time,Path,logout,ok),
   Logout is Time.


/*************************************************************************/
/*                  List Subroutines & Other Utilities                   */
/*************************************************************************/

make_list(String,List):- name(String,L1),append(X,[32|Y],L1),
   name(String1,X),
   make_list1(Y,[String1],List),!.
make_list(String,List):- name(String,L1),append(X,[Z|Y],L1),not(Z=32),
   List=[String],!.
make_list1(List,NewList,Ans):- append(X,[32|Y],List),
   name(String1,X),
   append(NewList,[String1],NewList1),
   make_list1(Y,NewList1,Ans),!.
make_list1(List,NewList,Ans):- append(X,[Z|Y],List),not(Z=32),
   name(String1,List),
   append(NewList,[String1],Ans),!.

make_path_list(String,List):- name(String,L1),append(X,[47|Y],L1),
   name(String1,X),
   make_path_list1(Y,[String1],List),!.
make_path_list(String,List):- name(String,L1),append(X,[Z|Y],L1),not(Z=47),
   List=[String],!.
make_path_list1(List,NewList,Ans):- append(X,[47|Y],List),
   name(String1,X),
   append(NewList,[String1],NewList1),
   make_path_list1(Y,NewList1,Ans),!.
make_path_list1(List,NewList,Ans):- append(X,[Z|Y],List),not(Z=47),
   name(String1,List),
   append(NewList,[String1],Ans),!.



tilde_word(Dir,Username):-
   name(Dir,L),
   first(L,126),
   append([X],List,L),
   name(Username,List).


get_times(List,T1,T2):- first(List,T1),last(List,T2).

first([First|List],First).
```

TAB 3. IDTS OPERATORS MODULE

```
/*****************************************************************************/
/* Intrusion-Detection Tutoring System Program -- Version 1        (IDTS)    */
/* LT Sandra J. Schiavo, U.S. Navy, Naval Postgraduate School, Monterey CA 93940 */
/*****************************************************************************/
/* IDTS Operators Module                                                     */
/*                                                                           */
/*    This module contains the four predicates required by the metutor30 module */
/* to tutor the student:                                                     */
/*                  recommended,                                             */
/*                  precondition,                                            */
/*                  postcondition,                                           */
/*                  deletepostcondition.                                     */
/*****************************************************************************/

/*****************************************************************************/
/*                              Recommended Facts                            */
/*****************************************************************************/

recommended([not(behavior(A,'edited password file',T1,T2))],
    [behavior(A,'edited password file',T1,T2)],
       restore(modified,file,passwd,from,backup)).
recommended([not(behavior(A,'copied password file',T1,T2))],
    [behavior(A,'copied password file',T1,T2)],
    change(permissions,file,passwd)).
recommended([not(behavior(A,'compromised root password',T1,T2))],
    [behavior(A,'compromised root password',T1,T2)],
    change(root,password)).
recommended([not(behavior(A,'inserted Trojan Horse',File,T1,T2))],
    [behavior(A,'inserted Trojan Horse',File,T1,T2)],
    remove('Trojan','Horse',from, File)).
recommended([not(behavior(A,'possible Trojan Horse',File,T1,T2))],
    [behavior(A,'possible Trojan Horse',File,T1,T2)],
    compare(file,File,for,'Trojan','Horse',with, File,on,backup,tape)).
recommended([not(behavior(A,'possible intruder',T1,T2))],
    [behavior(A,'possible intruder',T1,T2)],
    confront(user,A)).
recommended(
    [not(behavior(Intruder,'maliciously changed user password',User,T1,T2))],
    [behavior(Intruder,'maliciously changed user password',User,T1,T2)],
    restore(user,password,for,User)).
recommended(
    [not(behavior(A,'maliciously changed user password',T1,T2))],
    [behavior(A,'maliciously changed user password',T1,T2)],
    issue(A,new,user,password)).
recommended([not(behavior(A,'compromised user password',A,T1,T2))],
    [behavior(A,'compromised user password',A,T1,T2)],
    examine(user,password,A)).
recommended([not(behavior(A,'possible compromised user password',A,T1,T2))],
    [behavior(A,'possible compromised user password',A,T1,T2)],
    investigate(user,password,A)).
recommended([not(behavior(A,'maliciously modified file',X,T1,T2))],
    [behavior(A,'maliciously modified file',X,T1,T2)],
    restore(modified,file,X,from,backup)).
recommended([not(behavior(A,'maliciously deleted file',X,T1,T2))],
    [behavior(A,'maliciously deleted file',X,T1,T2)],
    restore(deleted,file,X,from,backup)).
recommended([checked(permissions,file,X)],check(permissions,file,X)).
recommended([executed(password,cracker)],execute(password,cracker)).
```

```
recommended([not(insecure_password(User))],
   [known(insecure,password,for,User)],
   change(password,for,User)).
recommended([found(file,X,on,backup,tape)],find(file,X,on,backup,tape)).
recommended([loaded(backup,tape)],load(backup,tape)).
recommended([located(backup,tape)],locate(backup,tape)).
recommended([stored(backup,tape)],store(backup,tape)).



/*****************************************************************************/
/*                              Preconditions                                */
/*****************************************************************************/

precondition(change(permissions,file,X),[not(changed(permissions,file,X)),
   checked(permissions,file,X)]).
precondition(change(root,password),
   [not(changed(password,root))]).
precondition(remove('Trojan','Horse',from, File),
   [restored(file,File)]).
precondition(compare(file,File,for,'Trojan','Horse',with,File,on,backup,tape),
   [found(file,File,on,backup,tape)]).
precondition(confront(user,A),
   [not(confronted(user,A))]).
precondition(restore(user,password,for,User),
   [not(restored(password,for,User))]).
precondition(issue(A,new,user,password),
   [not(issued(new,password,to,A))]).
precondition(examine(user,password,A),
   [not(examined(password,A))]).
precondition(investigate(user,password,A),
   [not(investigated(password,A))]).
precondition(restore(modified,file,X,from,backup),
   [found(file,X,on,backup,tape)]).
precondition(restore(deleted,file,X,from,backup),
   [found(file,X,on,backup,tape)]).
precondition(check(permissions,file,X), []).
precondition(execute(password,cracker),
   [not(executed(password,cracker))]).
precondition(change(password,for,User),[not(changed(password,for,User))]).
precondition(find(file,X,on,backup,tape),[loaded(backup,tape)]).
precondition(load(backup,tape),
   [not(loaded(backup,tape)),located(backup,tape)]).
precondition(locate(backup,tape),
   [not(located(backup,tape)),stored(backup,tape)]).
precondition(store(backup,tape),
   [not(stored(backup,tape))]).


/*****************************************************************************/
/*                        AddPostCondition Facts                             */
/*****************************************************************************/

addpostcondition(change(permissions,file,X),[changed(permissions,file,X)]).
addpostcondition(change(root,password),[changed(password,root)]).
addpostcondition(remove('Trojan','Horse',from, File),
   [removed('Trojan','Horse',from, File)]).
addpostcondition(
   compare(file,File,for,'Trojan','Horse',with,File,on,backup,tape),
   [compared(file,File,for,'Trojan Horse',with,File,on,backup,tape)]).
addpostcondition(confront(user,User),[confronted(user,User)]).
```

```
addpostcondition(restore(user,password,for,User),[restored(password,for,User)]).
addpostcondition(investigate(user,password,A),[investigated(user,password,A)]).
addpostcondition(examine(user,password,User),[examined(password,User)]).
addpostcondition(issue(User,new,user,password),[issued(new,password,to,User)]).
addpostcondition(check(permissions,file,X), [checked(permissions,file,X)]).
addpostcondition(restore(modified,file,X,from,backup),
   [modified_file(X,P,O,T,S,B,M)],
   [restored(file,X),file(X,P,O,T,S,B,M)]).
addpostcondition(restore(deleted,file,X,from,backup),
   [deleted_file(X,P,O,T,S,B,M)],
   [restored(file,X),file(X,P,O,T,S,B,M)]).
addpostcondition(execute(password,cracker),[insecure_password(User)],
   [executed(password,cracker),
   known(insecure,password,for,User1),
   known(insecure,password,for,User2),
   known(insecure,password,for,User3),
   known(insecure,password,for,User4)]).
addpostcondition(change(password,for,User),[changed(password,for,User)]).
addpostcondition(find(file,X,on,backup,tape),[found(file,X,on,backup,tape)]).
addpostcondition(load(backup,tape),[loaded(backup,tape)]).
addpostcondition(locate(backup,tape),[located(backup,tape)]).
addpostcondition(store(backup,tape),[stored(backup,tape)]).


/*****************************************************************************/
/*                          DeletePostCondition Facts                        */
/*****************************************************************************/

deletepostcondition(change(permissions,file,passwd),
   [behavior(A,'copied password file',T1,T2)]).
deletepostcondition(change(root,password),          /* 2 behaviors deleted */
   [behavior(A,'compromised root password',T1,T2),
   behavior(A1,'compromised root password',T3,T4)]).
deletepostcondition(remove('Trojan','Horse',from, File),
   [behavior(A,'inserted Trojan Horse',File,T1,T2)]).
deletepostcondition(
   compare(file,File,for,'Trojan','Horse',with,File,on,backup,tape),
   [behavior(A,'possible Trojan Horse',File,T1,T2)]).
deletepostcondition(confront(user,A),
   [behavior(A,'possible intruder',T1,T2)]).
deletepostcondition(investigate(user,password,A),
   [behavior(A,'possible compromised user password',A,T1,T2)]).
deletepostcondition(issue(A,new,user,password),
   [behavior(A,'maliciously changed user password',T1,T2)]).
deletepostcondition(restore(user,password,for,User),
   [behavior(Intruder,'maliciously changed user password',User,T1,T2)]).
deletepostcondition(examine(user,password,A),
   [behavior(A,'compromised user password',A,T1,T2)]).
deletepostcondition(restore(modified,file,passwd,from,backup),
   [modified_file(passwd,P,O,T,S,B,M),file(passwd,P,O,T,S1,B,M1),
   behavior(A,'edited password file',T1,T2)]).
deletepostcondition(restore(modified,file,X,from,backup),
   [modified_file(X,P,O,T,S,B,M),file(X,P,O,T,S1,B,M1),
   behavior(A,'maliciously modified file',X,T1,T2)]).
deletepostcondition(restore(deleted,file,X,from,backup),
   [deleted_file(X,P,O,T,S,B,M),
   behavior(A,'maliciously deleted file',X,T1,T2)]).
deletepostcondition(check(permissions,file,X), []).
deletepostcondition(execute(password,cracker),[]).
deletepostcondition(change(password,for,User),
   [insecure_password(User)]).
```

```
deletepostcondition(find(file,X,on,backup,tape),[]).
deletepostcondition(load(backup,tape),
   [removed(backup,tape)]).
deletepostcondition(locate(backup,tape),[stored(backup,tape)]).
deletepostcondition(store(backup,tape),
   [located(backup,tape),loaded(backup,tape)]).
```

TAB 4. IDTS FILES MODULE

```
/*****************************************************************************/
/* Intrusion-Detection Tutoring System (IDTS)                                */
/* LT Sandra J. Schiavo, U.S. Navy, Naval Postgraduate School, Monterey CA 93940 */
/*****************************************************************************/
/* IDTS Files Module                                                         */
/*                                                                           */
/*    This module contains file and insecure_password facts which store the  */
/* initial file system of IDTS's virtual environment.  The data structure of a */
/* file facts is as follows:                                                 */
/*                                                                           */
/*       file(<name>,<dir>,<owner>,<type>,<size>,<protection>,<time>).       */
/*                                                                           */
/* where, <name> is any legal UNIX file name;                                */
/*        <dir> is name of directory file <name> resides;                    */
/*        <owner> is name of owner of file <name>;                           */
/*        <type> is the file <name>'s type, either directory,text,or executable; */
/*        <size> is the size in bytes of file <name>;                        */
/*        <protection> are the UNIX permissions for file <name>; and         */
/*        <time> is the time file <name> was last modified by <owner>.       */
/*                                                                           */
/* The data structure for insecure_password is:                              */
/*                                                                           */
/*   insecure_password(<user>), where <user> is the name of user in the system. */
/*****************************************************************************/

:-dynamic file/7.

/*****************************************************************************/
/* Root directories and files.                                               */
/*****************************************************************************/

file(root,root,root,directory,100,'drwxr-xr-x',100).
file(bin,root,root,directory,100,'drwxr-sr-x',10).
file(users,root,root,directory,100,'drwxr-sr-x',10).
file(su,bin,root,executable,100,'-rwxr-xr-x',10).
file(ls,bin,root,executable,2000,'-rwxr-xr-x',20).
file(cd,bin,root,executable,5000,'-rwxr-xr-x',30).
file(etc,root,root,directory,100,'drwxr-sr-x',10).
file(passwd,etc,root,text,1000,'-rw-r--r--',40).


/*****************************************************************************/
/* Other Users and their files in the System.                                */
/*****************************************************************************/

file(adams,users,adams,directory,100,'drwxr-xr-x',100).
file(diradams,adams,adams,directory,512,'drwxr-xr-x',1002).
file(auxa,diradams,adams,text,1512,'-rw-r--r--',1000).
file(auxb,diradams,adams,text,1224,'-rw-r--r--',1234).
file(auxc,diradams,adams,text,5120,'-rw-r--r--',1515).

file(brown,users,brown,directory,100,'drwxr-xr-x',100).

file(coleman,users,coleman,directory,100,'drwxr-xr-x',100).

file(davis,users,davis,directory,100,'drwxr-xr-x',100).
file(goodnews,davis,davis,text,1348,'-rw-r--r--',2300).
```

```
file(doe,users,doe,directory,100,'drwxr-xr-x',100).
file(bigpaper,doe,doe,text,30000,'-rw-rw-rw-',500).

file(evans,users,evans,directory,100,'drwxr-xr-x',100).
file(csclass,evans,evans,directory,512,'drwxr-xr-x',2100).
file(proj_one,csclass,evans,exec,139268,'-rwxr--r--',0808).

file(farmer,users,farmer,directory,100,'drwxr-xr-x',100).
file(secrets,farmer,farmer,text,11348,'-rw-r--r--',1212).

file(graham,users,graham,directory,100,'drwxr-xr-x',100).
file(important,graham,graham,text,10248,'-rw-r--r--',1734).

file(jones,users,jones,directory,100,'drwxr-xr-x',100).

file(dog,users,dog,directory,100,'drwxr-xr-x',100).
file(food,dog,dog,text,1024,'-rw-r--r--',2210).
file(bark,dog,dog,text,1024,'-rw-r--r--',2210).
file(wag,dog,dog,text,1024,'-rw-r--r--',2210).

file(smith,users,smith,directory,100,'drwxr-xr-x',100).
file(shortpaper,smith,smith,text,5400,'-rw-rw-rw-',500).

file(tom,users,tom,directory,100,'drwxrwxrwx',100).
file(bb,tom,tom,text,512,'-rwxrwxrwx',1002).
file(aa,tom,tom,text,512,'-rwxrwxrwx',1002).
file(ba,tom,tom,directory,512,'drwxrwxrwx',1002).

file(uri,users,uri,directory,100,'drwxr-xr-x',100).
file(ba,uri,uri,directory,512,'drwxr-xr-x',1002).
file(baseball,ba,uri,text,512,'-rw-rw-r--',1002).


/*****************************************************************************/
/*   Insecure_password facts                                                 */
/*****************************************************************************/

insecure_password(adams).
insecure_password(graham).
insecure_password(farmer).
insecure_password(smith).
```

TAB 5. IDTS SAMPLE AUDITFILE MODULE

```
/*****************************************************************************/
/* Intrusion-Detection Tutoring System Program -- Version 1          (IDTS)  */
/* LT Sandra J. Schiavo, U.S. Navy, Naval Postgraduate School, Monterey CA 93940 */
/*****************************************************************************/
/* IDTS Sample Audit File -- auditfile                                       */
/*                                                                           */
/* This module contains sample audit facts that may be used by IDTS.        */
/* The data structure for an audit fact is as follows:                       */
/*                                                                           */
/*              audit(<user>,<time>,<directory>,<command>,<result>).         */
/*                                                                           */
/* where <user> is a user name on the system,                                */
/*       <time> is an integer and time <command> was executed                */
/*       <directory> is the <user>'s current directory where <command> executed */
/*       <command> is the UNIX command issued at <time> by <user>            */
/*       <result> is the result of executing <command>, and can be either, "ok," */
/*              "fail," an integer, or a mail message.                       */
/*****************************************************************************/

audit(adams,10,none,'login adams',ok).
audit(adams,30,none,'login adams',ok).
audit(adams,20,adams,ls,ok).
audit(adams,30,adams,'cd diradams',ok).
audit(adams,35,diradams,ls,ok).
audit(adams,40,diradams,'emacs auxa',1014).
audit(adams,50,diradams,'rm auxa',ok).
audit(adams,60,diradams,'emacs auxb',1212).
audit(adams,70,diradams,'rm auxb',ok).
audit(adams,80,diradams,'emacs auxc',1346).
audit(adams,90,diradams,'rm auxc',ok).
audit(adams,100,diradams,cd,ok).
audit(adams,110,adams,'rmdir diradams',ok).
audit(adams,120,adams,logout,ok).
audit(brown,130,none,'login brown',fail).
audit(brown,132,none,'login brown',fail).
audit(brown,134,none,'login brown',fail).
audit(brown,136,none,'login brown',ok).
audit(brown,138,brown,yppasswd,ok).
audit(brown,140,brown,logout,ok).
audit(coleman,160,none,'login coleman',fail).
audit(coleman,170,none,'login coleman',fail).
audit(coleman,180,none,'login coleman',fail).
audit(davis,190,none,'login davis',ok).
audit(davis,200,davis,'emacs goodnews',2372).
audit(root,315,none,'login root',fail).
audit(root,324,none,'login root',ok).
audit(root,329,root,'cd bin',ok).
audit(davis,410,davis,logout,ok).
audit(evans,420,none,'login evans',ok).
audit(evans,430,evans,ls,ok).
audit(evans,440,evans,'cd csclass',ok).
audit(evans,450,csclass,ls,ok).
audit(evans,460,csclass,'emacs proj_one',140292).
audit(root,589,bin,'emacs ls',3024).
audit(evans,880,csclass,logout,ok).
audit(smith,859,none,'login smith',ok).
audit(smith,900,smith,'cd etc',ok).
audit(smith,901,etc,'cp passwd ~smith',ok).
```

```
audit(smith,902,etc,logout,ok).
audit(jones,910,none,'login jones',ok).
audit(jones,910,jones,su,fail).
audit(jones,911,jones,su,fail).
audit(jones,912,jones,su,fail).
audit(jones,920,jones,su,ok).
audit(jones,921,root,'cd ~farmer',ok).
audit(jones,922,farmer,ls,ok).
audit(jones,923,farmer,'rm secrets',ok).
audit(jones,924,farmer,yppasswd,ok).
audit(jones,925,farmer,'cd ~graham',ok).
audit(jones,926,graham,ls,ok).
audit(jones,927,graham,'emacs important',11272).
audit(brown,1030,none,'login brown',fail).
audit(brown,1031,none,'login brown',fail).
audit(brown,1032,none,'login brown',fail).
audit(brown,1033,none,'mail root',bad(password,brown)).
audit(root,1119,bin,'emacs cd',4979).
audit(farmer,1203,none,'login farmer',fail).
audit(farmer,1204,none,'login farmer',fail).
audit(farmer,1205,none,'login farmer',fail).
audit(farmer,1206,none,'login farmer',fail).
audit(farmer,1207,farmer,'mail root',bad(password,farmer)).
audit(root,1211,root,mail,ok).
audit(farmer,1220,farmer,'mail root',bad(secrets,farmer)).
audit(root,1394,root,'cd ~dog',ok).
audit(root,1395,dog,'rm *',ok).
audit(root,1396,dog,cd,ok).
audit(root,1400,root,'login root',ok).
audit(root,1421,root,logout,ok).
audit(graham,1500,none,'login graham',ok).
audit(graham,1501,graham,ls,ok).
audit(graham,1502,graham,'mail root',bad(important,graham)).
audit(root,1503,root,mail,ok).
audit(uri,2119,none,'login uri',ok).
audit(uri,2127,uri,'cd ba',ok).
audit(uri,2216,ba,'rm *',ok).
audit(uri,2218,ba,logout,ok).
audit(tom,2713,none,'login tom',ok).
audit(tom,2732,tom,'cd ba',ok).
audit(tom,2749,ba,'cp aa guest/aa',ok).
audit(tom,2754,ba,logout,ok).
audit(root,4474,none,'login root',fail).
audit(root,4475,none,'login root',fail).
audit(root,4476,none,'login root',fail).
audit(root,4493,none,'login root',ok).
audit(root,4499,root,'cd etc',ok).
audit(root,5087,etc,'emacs passwd',1017).
audit(root,5088,etc,cd,ok).
audit(root,5089,root,'cd bin',ok).
audit(root,5205,bin,'mail root',bad(cd,bin)).
audit(root,5208,bin,logout,ok).
audit(tom,6351,none,'login tom',ok).
audit(tom,6355,tom,'cd ba',ok).
audit(tom,6421,ba,'emacs ab',12345).
audit(tom,6428,ba,logout,ok).
audit(doe,8982,none,'login doe',ok).
audit(doe,9315,doe,'emacs bigpaper',29947).
audit(doe,9335,doe,'emacs csproject',1024).
audit(doe,9352,doe,ls,ok).
audit(doe,9360,doe,'emacs csproject',4096).
```

```
audit(doe,9373,doe,'mail root',bad(ls,bin)).
audit(doe,9375,doe,'mail root',bad(doefile,doe)).
audit(doe,9379,doe,logout,ok).
audit(dog,9400,none,'login dog',ok).
audit(dog,9403,dog,ls,ok).
audit(dog,9404,dog,'mail root',bad(bark,dog)).
audit(dog,9405,dog,logout,ok).
```

APPENDIX B: SAMPLE SCRIPT RUNS WITH IDTS

The following are four script runs of IDTS using four different test audit files. The four different script runs are divided into the following appendix tabs:

Tab 1. Test Auditfile 1
Tab 2. Test Auditfile 2
Tab 3. Test Auditfile 3
Tab 4. Test Auditfile 4

TAB 1. TEST AUDITFILE 1

The following is the audit file used for Run 1:

```
audit(adams,10,none,'login adams',ok).
audit(adams,30,none,'login adams',ok).
audit(adams,20,adams,ls,ok).
audit(adams,30,adams,'cd diradams',ok).
audit(adams,35,diradams,ls,ok).
audit(adams,40,diradams,'emacs auxa',1014).
audit(adams,50,diradams,'rm auxa',ok).
audit(adams,60,diradams,'emacs auxb',1212).
audit(adams,70,diradams,'rm auxb',ok).
audit(adams,80,diradams,'emacs auxc',1346).
audit(adams,90,diradams,'rm auxc',ok).
audit(adams,100,diradams,cd,ok).
audit(adams,110,adams,'rmdir diradams',ok).
audit(adams,120,adams,logout,ok).
audit(brown,130,none,'login brown',fail).
audit(brown,132,none,'login brown',fail).
audit(brown,134,none,'login brown',fail).
audit(brown,136,none,'login brown',ok).
audit(brown,138,brown,yppasswd,ok).
audit(brown,140,brown,logout,ok).
audit(coleman,160,none,'login coleman',fail).
audit(coleman,170,none,'login coleman',fail).
audit(coleman,180,none,'login coleman',fail).
audit(davis,190,none,'login davis',ok).
audit(davis,200,davis,'emacs goodnews',2372).
audit(root,315,none,'login root',fail).
audit(root,324,none,'login root',ok).
audit(root,329,root,'cd bin',ok).
audit(davis,410,davis,logout,ok).
audit(evans,420,none,'login evans',ok).
audit(evans,430,evans,ls,ok).
audit(evans,440,evans,'cd csclass',ok).
audit(evans,450,csclass,ls,ok).
audit(evans,460,csclass,'emacs proj_one',140292).
audit(root,589,bin,'emacs ls',3024).
audit(evans,880,csclass,logout,ok).
audit(smith,859,none,'login smith',ok).
audit(smith,900,smith,'cd etc',ok).
audit(smith,901,etc,'cp passwd ~smith',ok).
audit(smith,902,etc,logout,ok).
audit(jones,910,none,'login jones',ok).
audit(jones,910,jones,su,fail).
audit(jones,911,jones,su,fail).
audit(jones,912,jones,su,fail).
audit(jones,920,jones,su,ok).
audit(jones,921,root,'cd ~farmer',ok).
audit(jones,922,farmer,ls,ok).
audit(jones,923,farmer,'rm secrets',ok).
audit(jones,924,farmer,yppasswd,ok).
audit(jones,925,farmer,'cd ~graham',ok).
audit(jones,926,graham,ls,ok).
audit(jones,927,graham,'emacs important',11272).
audit(brown,1030,none,'login brown',fail).
audit(brown,1031,none,'login brown',fail).
```

```
audit(brown,1032,none,'login brown',fail).
audit(brown,1033,none,'mail root',bad(password,brown)).
audit(root,1119,bin,'emacs cd',4979).
audit(farmer,1203,none,'login farmer',fail).
audit(farmer,1204,none,'login farmer',fail).
audit(farmer,1205,none,'login farmer',fail).
audit(farmer,1206,none,'login farmer',fail).
audit(farmer,1207,farmer,'mail root',bad(password,farmer)).
audit(root,1211,root,mail,ok).
audit(farmer,1220,farmer,'mail root',bad(secrets,farmer)).
audit(root,1394,root,'cd ~dog',ok).
audit(root,1395,dog,'rm *',ok).
audit(root,1396,dog,cd,ok).
audit(root,1400,root,'login root',ok).
audit(root,1421,root,logout,ok).
audit(graham,1500,none,'login graham',ok).
audit(graham,1501,graham,ls,ok).
audit(graham,1502,graham,'mail root',bad(important,graham)).
audit(root,1503,root,mail,ok).
audit(uri,2119,none,'login uri',ok).
audit(uri,2127,uri,'cd ba',ok).
audit(uri,2216,ba,'rm *',ok).
audit(uri,2218,ba,logout,ok).
audit(tom,2713,none,'login tom',ok).
audit(tom,2732,tom,'cd ba',ok).
audit(tom,2749,ba,'cp aa guest/aa',ok).
audit(tom,2754,ba,logout,ok).
audit(root,4474,none,'login root',fail).
audit(root,4475,none,'login root',fail).
audit(root,4476,none,'login root',fail).
audit(root,4493,none,'login root',ok).
audit(root,4499,root,'cd etc',ok).
audit(root,5087,etc,'emacs passwd',1017).
audit(root,5088,etc,cd,ok).
audit(root,5089,root,'cd bin',ok).
audit(root,5205,bin,'mail root',bad(cd,bin)).
audit(root,5208,bin,logout,ok).
audit(tom,6351,none,'login tom',ok).
audit(tom,6355,tom,'cd ba',ok).
audit(tom,6421,ba,'emacs ab',12345).
audit(tom,6428,ba,logout,ok).
audit(doe,8982,none,'login doe',ok).
audit(doe,9315,doe,'emacs bigpaper',29947).
audit(doe,9335,doe,'emacs csproject',1024).
audit(doe,9352,doe,ls,ok).
audit(doe,9360,doe,'emacs csproject',4096).
audit(doe,9373,doe,'mail root',bad(ls,bin)).
audit(doe,9375,doe,'mail root',bad(doefile,doe)).
audit(doe,9379,doe,logout,ok).
audit(dog,9400,none,'login dog',ok).
audit(dog,9403,dog,ls,ok).
audit(dog,9404,dog,'mail root',bad(bark,dog)).
audit(dog,9405,dog,logout,ok).
```

The following is the script of Run 1:

```
Script started on Thu Mar 16 00:16:45 1995
.alias: No such file or directory.
[7mai2:/users/work4/schiavo/Thesis/Tutor>>[mprolog


Quintus Prolog Release 3.1.1 (Sun-4, SunOS 4.0)
Copyright (C) 1990, Quintus Corporation.  All rights reserved.
2100 Geng Road, Palo Alto, California U.S.A. (415) 813-3800

| ?- [intruder].
% compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/intruder.pl
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/metutor30.pl
% Undefined procedures will just fail ('fail' option)
%   loading file /usr/local/q3.1.1/generic/qplib3.1.1/library/random.qof
%    foreign file /usr/local/q3.1.1/generic/qplib3.1.1/library/sun4-4/libpl.so loaded
%   random.qof loaded, 0.134 sec 9,392 bytes
%   module random imported into user
* Clauses for writefact/2 are not together in the source file
%  metutor30.pl compiled in module user, 3.367 sec 50,420 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/auditfile
%  auditfile compiled in module user, 0.417 sec 8,744 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/filetree
%  filetree compiled in module user, 0.467 sec 5,240 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/rules
* Clauses for behavior/5 are not together in the source file
* Clauses for behavior/4 are not together in the source file
%  rules compiled in module user, 0.666 sec 7,416 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/files
%  files compiled in module user, 0.117 sec 4,276 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/operators
* Clauses for recommended/3 are not together in the source file
* Clauses for recommended/2 are not together in the source file
* Clauses for addpostcondition/2 are not together in the source file
%  operators compiled in module user, 0.583 sec 8,268 bytes
% intruder.pl compiled in module user, 6.383 sec 95,212 bytes

yes
| ?- statistics.

memory (total)          649696 bytes:     458764 in use,     190932 free
   program space        327700 bytes
   global space          65532 bytes:      26688 in use,      38844 free
      global stack                         24584 bytes
      trail                                   16 bytes
      system                                2088 bytes
   local stack           65532 bytes:        440 in use,      65092 free
      local stack                           416 bytes
      system                                 24 bytes

 0.000 sec. for 0 global and 3 local space shifts
 0.000 sec. for 0 garbage collections which collected 0 bytes
 5.933 sec. runtime

yes
| ?- start.
```

```
*******************************************************************************
*                                                                             *
*                                AUDIT FILE                                   *
*                                                                             *
*      The following displays the current contents of the audit file:         *
*                                                                             *
*******************************************************************************
```

Name	Time	Path	Command	Result
adams	10	none	login adams	ok
adams	20	adams	ls	ok
adams	30	adams	cd diradams	ok
adams	30	none	login adams	ok
adams	35	diradams	ls	ok
adams	40	diradams	emacs auxa	1014
adams	50	diradams	rm auxa	ok
adams	60	diradams	emacs auxb	1212
adams	70	diradams	rm auxb	ok
adams	80	diradams	emacs auxc	1346
adams	90	diradams	rm auxc	ok
adams	100	diradams	cd	ok
adams	110	adams	rmdir diradams	ok
adams	120	adams	logout	ok
brown	130	none	login brown	fail
brown	132	none	login brown	fail
brown	134	none	login brown	fail
brown	136	none	login brown	ok
brown	138	brown	yppasswd	ok
brown	140	brown	logout	ok
brown	1030	none	login brown	fail
brown	1031	none	login brown	fail
brown	1032	none	login brown	fail
brown	1033	none	mail root	bad(password,brown)
coleman	160	none	login coleman	fail
coleman	170	none	login coleman	fail
coleman	180	none	login coleman	fail
davis	190	none	login davis	ok
davis	200	davis	emacs goodnews	2372
davis	410	davis	logout	ok
doe	8982	none	login doe	ok
doe	9315	doe	emacs bigpaper	29947
doe	9335	doe	emacs csproject	1024
doe	9352	doe	ls	ok
doe	9360	doe	emacs csproject	4096
doe	9373	doe	mail root	bad(ls,bin)
doe	9375	doe	mail root	bad(doefile,doe)
doe	9379	doe	logout	ok
dog	9400	none	login dog	ok
dog	9403	dog	ls	ok
dog	9404	dog	mail root	bad(bark,dog)
dog	9405	dog	logout	ok
evans	420	none	login evans	ok
evans	430	evans	ls	ok
evans	440	evans	cd csclass	ok
evans	450	csclass	ls	ok
evans	460	csclass	emacs proj_one	140292
evans	880	csclass	logout	ok
farmer	1203	none	login farmer	fail
farmer	1204	none	login farmer	fail

farmer	1205	none	login farmer	fail
farmer	1206	none	login farmer	fail
farmer	1207	farmer	mail root	bad(password,farmer)
farmer	1220	farmer	mail root	bad(secrets,farmer)
graham	1500	none	login graham	ok
graham	1501	graham	ls	ok
graham	1502	graham	mail root	bad(important,graham)
jones	910	jones	su	fail
jones	910	none	login jones	ok
jones	911	jones	su	fail
jones	912	jones	su	fail
jones	920	jones	su	ok
jones	921	root	cd ~farmer	ok
jones	922	farmer	ls	ok
jones	923	farmer	rm secrets	ok
jones	924	farmer	yppasswd	ok
jones	925	farmer	cd ~graham	ok
jones	926	graham	ls	ok
jones	927	graham	emacs important	11272
root	315	none	login root	fail
root	324	none	login root	ok
root	329	root	cd bin	ok
root	589	bin	emacs ls	3024
root	1119	bin	emacs cd	4979
root	1211	root	mail	ok
root	1394	root	cd ~dog	ok
root	1395	dog	rm *	ok
root	1396	dog	cd	ok
root	1400	root	login root	ok
root	1421	root	logout	ok
root	1503	root	mail	ok
root	4474	none	login root	fail
root	4475	none	login root	fail
root	4476	none	login root	fail
root	4493	none	login root	ok
root	4499	root	cd etc	ok
root	5087	etc	emacs passwd	1017
root	5088	etc	cd	ok
root	5089	root	cd bin	ok
root	5205	bin	mail root	bad(cd,bin)
root	5208	bin	logout	ok
smith	859	none	login smith	ok
smith	900	smith	cd etc	ok
smith	901	etc	cp passwd ~smith	ok
smith	902	etc	logout	ok
tom	2713	none	login tom	ok
tom	2732	tom	cd ba	ok
tom	2749	ba	cp aa guest/aa	ok
tom	2754	ba	logout	ok
tom	6351	none	login tom	ok
tom	6355	tom	cd ba	ok
tom	6421	ba	emacs ab	12345
tom	6428	ba	logout	ok
uri	2119	none	login uri	ok
uri	2127	uri	cd ba	ok
uri	2216	ba	rm *	ok
uri	2218	ba	logout	ok

```
*****************************************************************************
*                                                                           *
*                                MAIL RECEIVED                              *
*                                                                           *
*      The following displays mail received by root:                        *
*                                                                           *
*****************************************************************************


From        To      Time       Problem(File,Directory)

brown       root    1033       bad(password,brown)
doe         root    9373       bad(ls,bin)
doe         root    9375       bad(doefile,doe)
dog         root    9404       bad(bark,dog)
farmer      root    1207       bad(password,farmer)
farmer      root    1220       bad(secrets,farmer)
graham      root    1502       bad(important,graham)
root        root    5205       bad(cd,bin)

% Undefined procedures will just fail ('fail' option)
Warnings:
This fact is not removable: changed(password,root)
This fact is not removable: confronted(user,_14117)
This fact is not removable: examined(password,_14051)
This fact is not removable: executed(password,cracker)
This fact is not removable: investigated(password,_14030)
This fact is not removable: changed(password,for,_13988)
This fact is not removable: changed(permissions,file,_14160)
This fact is not removable: restored(password,for,_14096)
This fact is not removable: issued(new,password,to,_14074)

Your objectives:
backup tape is stored and password cracker is executed.
Wait a moment while I analyze the problem thoroughly.

*************************************************************************
*                                                                       *
*  To see a list of possible actions, type the letter "h" or the word   *
*  "help." To review the audit file or your mail at anytime, type the   *
*  word "auditfile" or "mail" respectively.                             *
*                                                                       *
*************************************************************************
Type h for help.
************ These facts are now true: *************
backup tape is stored,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
and mail(root,root,5205,bad(cd,bin)) is true.
Select an action: execute password cracker
You chose to execute password cracker.
I am thinking....
OK, but a hint: "restore modified file passwd from backup"
 is more important now than "execute password cracker".
************ These facts are now true: *************
password cracker is executed,
```

```
backup tape is stored,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
and mail(root,root,5205,bad(cd,bin)) is true.
Select an action: restore modified file passwd from backup
You chose to restore modified file passwd from backup.
>>>>Operator restore(modified,file,passwd,from,backup) could not be applied to:
password cracker is executed,
backup tape is stored,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
and mail(root,root,5205,bad(cd,bin)) is true
>>>>Operator restore(modified,file,passwd,from,backup) could not be applied to:
password cracker is executed,
backup tape is stored,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
and mail(root,root,5205,bad(cd,bin)) is true
That action requires that:
found(file,passwd,on,backup,tape) is true.
************ These facts are now true: *************
password cracker is executed,
backup tape is stored,
known(insecure,password,for,_323991) is true,
known(insecure,password,for,_323998) is true,
known(insecure,password,for,_324005) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
and mail(root,root,5205,bad(cd,bin)) is true.
Select an action: find file passwd on backup tape
You chose to find file passwd on backup tape.
>>>>Operator find(file,passwd,on,backup,tape) could not be applied to:
password cracker is executed,
backup tape is stored,
known(insecure,password,for,adams) is true,
```

```
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
and mail(root,root,5205,bad(cd,bin)) is true
>>>>Operator find(file,passwd,on,backup,tape) could not be applied to:
password cracker is executed,
backup tape is stored,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
and mail(root,root,5205,bad(cd,bin)) is true
Have you confused "backup tape is loaded" with "backup tape is stored"?
That action requires that:
backup tape must be loaded.
************ These facts are now true: *************
password cracker is executed,
backup tape is stored,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
and mail(root,root,5205,bad(cd,bin)) is true.
Select an action: load backup tape
You chose to load backup tape.
>>>>Operator load(backup,tape) could not be applied to:
password cracker is executed,
backup tape is stored,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
and mail(root,root,5205,bad(cd,bin)) is true
>>>>Operator load(backup,tape) could not be applied to:
password cracker is executed,
backup tape is stored,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
```

```
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
and mail(root,root,5205,bad(cd,bin)) is true
Have you confused "backup tape is located" with "backup tape is stored"?
Have you confused that with the locate backup tape action?
That action requires that:
backup tape must be located.
************ These facts are now true: *************
password cracker is executed,
backup tape is stored,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
and mail(root,root,5205,bad(cd,bin)) is true.
Select an action: locate backup tape
You chose to locate backup tape.
OK.
************ These facts are now true: *************
password cracker is executed,
backup tape is located,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
and mail(root,root,5205,bad(cd,bin)) is true.
Select an action: load backup tape
You chose to load backup tape.
OK.
************ These facts are now true: *************
password cracker is executed,
backup tape is loaded,
backup tape is located,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
and mail(root,root,5205,bad(cd,bin)) is true.
Select an action: find file passwd on backup tape
You chose to find file passwd on backup tape.
OK.
************ These facts are now true: *************
password cracker is executed,
backup tape is loaded,
```

```
backup tape is located,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
and found(file,passwd,on,backup,tape) is true.
Select an action: restore modified file passwd from backup
You chose to restore modified file passwd from backup.
OK.
************ These facts are now true: *************
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
and found(file,passwd,on,backup,tape) is true.
Select an action: change password for adams
You chose to change password for adams.
I am thinking....
OK, but a hint: "change permissions file passwd"
 is more important now than "change password for adams".
************ These facts are now true: *************
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
and found(file,passwd,on,backup,tape) is true.
Select an action: change permissions file passwd
I am thinking....
You chose to change permissions file passwd.
>>>>Operator change(permissions,file,passwd) could not be applied to:
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
```

```
changed(password,for,adams) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
and found(file,passwd,on,backup,tape) is true
>>>>Operator change(permissions,file,passwd) could not be applied to:
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
and found(file,passwd,on,backup,tape) is true
Have you confused that with the check permissions file passwd action?
That action requires that:
checked(permissions,file,passwd) is true.
************ These facts are now true: *************
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
and found(file,passwd,on,backup,tape) is true.
Select an action: check permissions file passwd
You chose to check permissions file passwd.
OK.
************ These facts are now true: *************
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
```

```
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
and found(file,passwd,on,backup,tape) is true.
Select an action: change permissions file passwd
You chose to change permissions file passwd.
OK.
************ These facts are now true: *************
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
and found(file,passwd,on,backup,tape) is true.
Select an action: change password for smith
You chose to change password for smith.
I am thinking....
OK, but a hint: "change root password"
 is more important now than "change password for smith".
************ These facts are now true: *************
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
and found(file,passwd,on,backup,tape) is true.
Select an action: change root password
You chose to change root password.
OK.
************ These facts are now true: *************
password root is changed,
```

```
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
and found(file,passwd,on,backup,tape) is true.
Select an action: auditfile

*******************************************************************************
*                                                                             *
*                                 AUDIT FILE                                  *
*                                                                             *
*      The following displays the current contents of the audit file:         *
*                                                                             *
*******************************************************************************

Name       Time     Path          Command        Result

adams        10     none        login adams      ok
adams        20     adams             ls         ok
adams        30     adams       cd diradams      ok
adams        30     none        login adams      ok
adams        35     diradams          ls         ok
adams        40     diradams     emacs auxa      1014
adams        50     diradams        rm auxa      ok
adams        60     diradams     emacs auxb      1212
adams        70     diradams        rm auxb      ok
adams        80     diradams     emacs auxc      1346
adams        90     diradams        rm auxc      ok
adams       100     diradams          cd         ok
adams       110     adams      rmdir diradams    ok
adams       120     adams           logout       ok
brown       130     none         login brown     fail
brown       132     none         login brown     fail
brown       134     none         login brown     fail
brown       136     none         login brown     ok
brown       138     brown          yppasswd      ok
brown       140     brown            logout      ok
brown      1030     none         login brown     fail
brown      1031     none         login brown     fail
brown      1032     none         login brown     fail
brown      1033     none           mail root     bad(password,brown)
coleman     160     none        login coleman    fail
coleman     170     none        login coleman    fail
coleman     180     none        login coleman    fail
davis       190     none          login davis    ok
davis       200     davis     emacs goodnews     2372
```

davis	410	davis	logout	ok
doe	8982	none	login doe	ok
doe	9315	doe	emacs bigpaper	29947
doe	9335	doe	emacs csproject	1024
doe	9352	doe	ls	ok
doe	9360	doe	emacs csproject	4096
doe	9373	doe	mail root	bad(ls,bin)
doe	9375	doe	mail root	bad(doefile,doe)
doe	9379	doe	logout	ok
dog	9400	none	login dog	ok
dog	9403	dog	ls	ok
dog	9404	dog	mail root	bad(bark,dog)
dog	9405	dog	logout	ok
evans	420	none	login evans	ok
evans	430	evans	ls	ok
evans	440	evans	cd csclass	ok
evans	450	csclass	ls	ok
evans	460	csclass	emacs proj_one	140292
evans	880	csclass	logout	ok
farmer	1203	none	login farmer	fail
farmer	1204	none	login farmer	fail
farmer	1205	none	login farmer	fail
farmer	1206	none	login farmer	fail
farmer	1207	farmer	mail root	bad(password,farmer)
farmer	1220	farmer	mail root	bad(secrets,farmer)
graham	1500	none	login graham	ok
graham	1501	graham	ls	ok
graham	1502	graham	mail root	bad(important,graham)
jones	910	jones	su	fail
jones	910	none	login jones	ok
jones	911	jones	su	fail
jones	912	jones	su	fail
jones	920	jones	su	ok
jones	921	root	cd ~farmer	ok
jones	922	farmer	ls	ok
jones	923	farmer	rm secrets	ok
jones	924	farmer	yppasswd	ok
jones	925	farmer	cd ~graham	ok
jones	926	graham	ls	ok
jones	927	graham	emacs important	11272
root	315	none	login root	fail
root	324	none	login root	ok
root	329	root	cd bin	ok
root	589	bin	emacs ls	3024
root	1119	bin	emacs cd	4979
root	1211	root	mail	ok
root	1394	root	cd ~dog	ok
root	1395	dog	rm *	ok
root	1396	dog	cd	ok
root	1400	root	login root	ok
root	1421	root	logout	ok
root	1503	root	mail	ok
root	4474	none	login root	fail
root	4475	none	login root	fail
root	4476	none	login root	fail
root	4493	none	login root	ok
root	4499	root	cd etc	ok
root	5087	etc	emacs passwd	1017
root	5088	etc	cd	ok
root	5089	root	cd bin	ok
root	5205	bin	mail root	bad(cd,bin)

```
root        5208      bin                 logout      ok
smith        859      none           login smith      ok
smith        900      smith               cd etc      ok
smith        901      etc       cp passwd ~smith      ok
smith        902      etc                 logout      ok
tom         2713      none           login tom        ok
tom         2732      tom                 cd ba       ok
tom         2749      ba           cp aa guest/aa     ok
tom         2754      ba                  logout      ok
tom         6351      none           login tom        ok
tom         6355      tom                 cd ba       ok
tom         6421      ba                emacs ab      12345
tom         6428      ba                  logout      ok
uri         2119      none           login uri        ok
uri         2127      uri                 cd ba       ok
uri         2216      ba                   rm *       ok
uri         2218      ba                  logout      ok

************ These facts are now true: *************
password root is changed,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
and found(file,passwd,on,backup,tape) is true.
Select an action: mail

*******************************************************************************
*                                                                             *
*                                 MAIL RECEIVED                               *
*                                                                             *
*      The following displays mail received by root:                          *
*                                                                             *
*******************************************************************************

From        To        Time        Problem(File,Directory)

brown       root      1033        bad(password,brown)
doe         root      9373        bad(ls,bin)
doe         root      9375        bad(doefile,doe)
dog         root      9404        bad(bark,dog)
farmer      root      1207        bad(password,farmer)
farmer      root      1220        bad(secrets,farmer)
graham      root      1502        bad(important,graham)
root        root      5205        bad(cd,bin)
```

```
************ These facts are now true: *************
password root is changed,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
and found(file,passwd,on,backup,tape) is true.
Select an action: confront user jones
You chose to confront user jones.
OK, but a hint: "compare file cd for Trojan Horse with cd on backup tape"
 is more important now than "confront user jones".
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
and found(file,passwd,on,backup,tape) is true.
Select an action: find file cd on backup tape
You chose to find file cd on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
```

```
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
and found(file,passwd,on,backup,tape) is true.
Select an action: compare file cd for Trojan Horse with cd on backup tape
You chose to compare file cd for Trojan Horse with cd on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
and compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true.
Select an action: find file ls on backup tape
You chose to find file ls on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
```

```
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
and compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true.
Select an action: compare file ls for Trojan Horse with ls on backup tape
You chose to compare file ls for Trojan Horse with ls on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: remove Trojan Horse from ls
You chose to remove Trojan Horse from ls.
>>>>Operator remove(Trojan,Horse,from,ls) could not be applied to:
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
```

```
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true
>>>>Operator remove(Trojan,Horse,from,ls) could not be applied to:
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true
Have you confused "file ls are restored" with "file passwd is restored"?
That action requires that:
file ls must be restored.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore modified file ls from backup
You chose to restore modified file ls from backup.
I am thinking....
OK, but a hint: "restore user password for brown"
```

```
 is more important now than "restore modified file ls from backup".
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: remove Trojan Horse from ls
You chose to remove Trojan Horse from ls.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore user password brown
You chose to restore user password brown.
```

```
Not a valid action.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore user password for brown
You chose to restore user password for brown.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
restored(password,for,brown) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
```

```
Select an action: restore user password for root
You chose to restore user password for root.
I am thinking....
Have you confused that with the restore user password for farmer action?
Your action is not what I would choose, but let us try it.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
restored(password,for,brown) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore user password for farmer
You chose to restore user password for farmer.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
```

```
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: examine user password adams
You chose to examine user password adams.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password adams is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: examine user password root
You chose to examine user password root.
I am thinking....
Your action is not what I would choose, but let us try it.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password adams is examined,
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
```

```
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: investigate user password root
You chose to investigate user password root.
Have you confused that with the investigate user password brown action?
OK, but a hint: "investigate user password brown"
 is more important now than "investigate user password root".
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password adams is examined,
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,root) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: investigate user password brown
You chose to investigate user password brown.
OK.
```

```
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password adams is examined,
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,brown) is true,
investigated(user,password,root) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore modified file cd from backup
You chose to restore modified file cd from backup.
OK, but a hint: "restore modified file important from backup"
 is more important now than "restore modified file cd from backup".
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password adams is examined,
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file cd is restored,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,brown) is true,
investigated(user,password,root) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
```

```
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: find file important on backup tape
You chose to find file important on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password adams is examined,
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file cd is restored,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,brown) is true,
investigated(user,password,root) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,important,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore modified file important from backup
You chose to restore modified file important from backup.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password adams is examined,
```

```
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file cd is restored,
file important is restored,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,brown) is true,
investigated(user,password,root) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,important,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: find file wag on backup tape
You chose to find file wag on backup tape.
I am thinking....
Have you confused that with the find file secrets on backup tape action?
OK, but a hint: "restore deleted file secrets from backup"
 is more important now than "restore deleted file wag from backup".
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password adams is examined,
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file cd is restored,
file important is restored,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,brown) is true,
investigated(user,password,root) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
```

```
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,important,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
found(file,wag,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: find file secrets on backup tape
You chose to find file secrets on backup tape.
OK.
********** These facts are now true: **********
password root is changed,
user jones is confronted,
password adams is examined,
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file cd is restored,
file important is restored,
file ls are restored,
file passwd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,brown) is true,
investigated(user,password,root) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,important,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
found(file,secrets,on,backup,tape) is true,
found(file,wag,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
```

```
Select an action: restore deleted file secrets from backup
You chose to restore deleted file secrets from backup.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password adams is examined,
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file cd is restored,
file important is restored,
file ls are restored,
file passwd is restored,
file secrets are restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,brown) is true,
investigated(user,password,root) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,important,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
found(file,secrets,on,backup,tape) is true,
found(file,wag,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore deleted file wag from backup
You chose to restore deleted file wag from backup.
OK, but a hint: "restore deleted file bark from backup"
 is more important now than "restore deleted file wag from backup".
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password adams is examined,
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file cd is restored,
file important is restored,
file ls are restored,
file passwd is restored,
file secrets are restored,
```

```
file wag is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,brown) is true,
investigated(user,password,root) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,cd,on,backup,tape) is true,
found(file,important,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
found(file,secrets,on,backup,tape) is true,
found(file,wag,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: find file bark on backup tape
You chose to find file bark on backup tape.
OK.
************ These facts are now true: **************
password root is changed,
user jones is confronted,
password adams is examined,
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file cd is restored,
file important is restored,
file ls are restored,
file passwd is restored,
file secrets are restored,
file wag is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,brown) is true,
investigated(user,password,root) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
```

```
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,bark,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,important,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
found(file,secrets,on,backup,tape) is true,
found(file,wag,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore deleted file bark from backup
You chose to restore deleted file bark from backup.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password adams is examined,
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file bark is restored,
file cd is restored,
file important is restored,
file ls are restored,
file passwd is restored,
file secrets are restored,
file wag is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,brown) is true,
investigated(user,password,root) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,bark,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,important,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
found(file,secrets,on,backup,tape) is true,
found(file,wag,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
```

```
Select an action: find file food on backup tape
You chose to find file food on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password adams is examined,
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file bark is restored,
file cd is restored,
file important is restored,
file ls are restored,
file passwd is restored,
file secrets are restored,
file wag is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,brown) is true,
investigated(user,password,root) is true,
restored(password,for,brown) is true,
restored(password,for,farmer) is true,
restored(password,for,root) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,1033,bad(password,brown)) is true,
mail(doe,root,9373,bad(ls,bin)) is true,
mail(doe,root,9375,bad(doefile,doe)) is true,
mail(dog,root,9404,bad(bark,dog)) is true,
mail(farmer,root,1207,bad(password,farmer)) is true,
mail(farmer,root,1220,bad(secrets,farmer)) is true,
mail(graham,root,1502,bad(important,graham)) is true,
mail(root,root,5205,bad(cd,bin)) is true,
removed(Trojan,Horse,from,ls) is true,
found(file,bark,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,food,on,backup,tape) is true,
found(file,important,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
found(file,passwd,on,backup,tape) is true,
found(file,secrets,on,backup,tape) is true,
found(file,wag,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore deleted file food from backup
You chose to restore deleted file food from backup.
OK.
************ These facts are now true: *************
password root is changed,
user jones is confronted,
password adams is examined,
password root is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file bark is restored,
file cd is restored,
```

```
 file food is restored,
 file important is restored,
 file ls are restored,
 file passwd is restored,
 file secrets are restored,
 file wag is restored,
 changed(password,for,adams) is true,
 changed(password,for,smith) is true,
 changed(permissions,file,passwd) is true,
 checked(permissions,file,passwd) is true,
 investigated(user,password,brown) is true,
 investigated(user,password,root) is true,
 restored(password,for,brown) is true,
 restored(password,for,farmer) is true,
 restored(password,for,root) is true,
 known(insecure,password,for,adams) is true,
 known(insecure,password,for,smith) is true,
 mail(brown,root,1033,bad(password,brown)) is true,
 mail(doe,root,9373,bad(ls,bin)) is true,
 mail(doe,root,9375,bad(doefile,doe)) is true,
 mail(dog,root,9404,bad(bark,dog)) is true,
 mail(farmer,root,1207,bad(password,farmer)) is true,
 mail(farmer,root,1220,bad(secrets,farmer)) is true,
 mail(graham,root,1502,bad(important,graham)) is true,
 mail(root,root,5205,bad(cd,bin)) is true,
 removed(Trojan,Horse,from,ls) is true,
 found(file,bark,on,backup,tape) is true,
 found(file,cd,on,backup,tape) is true,
 found(file,food,on,backup,tape) is true,
 found(file,important,on,backup,tape) is true,
 found(file,ls,on,backup,tape) is true,
 found(file,passwd,on,backup,tape) is true,
 found(file,secrets,on,backup,tape) is true,
 found(file,wag,on,backup,tape) is true,
 compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
 and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
 Select an action: store backup tape
 You chose to store backup tape.
 OK.
 Congratulations! You have done the job.
 The session is over.  Do "go." to restart.

yes
| ?- statistics.

memory (total)          4188640 bytes:    2743656 in use,    1444984 free
   program space        2612592 bytes
   global space           65532 bytes:      26644 in use,      38888 free
      global stack                          24516 bytes
      trail                                    40 bytes
      system                                 2088 bytes
   local stack            65532 bytes:        648 in use,      64884 free
      local stack                           624 bytes
      system                                 24 bytes

 67.000 sec. for 0 global and 45 local space shifts
 0.834 sec. for 3 garbage collections which collected 2905820 bytes
 87.633 sec. runtime

yes
| ?- halt.
```

TAB 2. RUN 2

The following is the audit file used for Run 2:

```
audit(davis,9,none,'login davis',ok).
audit(davis,14,davis,'cd ~adams',ok).
audit(davis,21,adams,ls,ok).
audit(davis,96,adams,'login adams',fail).
audit(davis,108,adams,'login adams',ok).
audit(adams,122,adams,'cd ~adams',ok).
audit(adams,125,adams,'cd diradams',ok).
audit(evans,340,none,'login evans',ok).
audit(adams,500,diradams,'emacs auxb',1229).
audit(coleman,622,none,'login coleman',fail).
audit(evans,625,evans,'emacs csclass',511).
audit(coleman,632,none,'login coleman',fail).
audit(coleman,636,none,'login coleman',ok).
audit(coleman,652,coleman,'cd ~smith',ok).
audit(evans,655,evans,'mail root',bad(csclass,evans)).
audit(evans,657,evans,logout,ok).
audit(farmer,668,farmer,'cd ~root/bin',ok).
audit(farmer,668,none,'login farmer',ok).
audit(farmer,671,bin,ls,ok).
audit(coleman,684,smith,ls,ok).
audit(farmer,687,bin,'cd ~root',ok).
audit(farmer,707,root,ls,ok).
audit(farmer,711,root,'login root',fail).
audit(farmer,716,root,'login root',fail).
audit(farmer,720,root,'login root',fail).
audit(farmer,722,root,'login root',fail).
audit(coleman,729,smith,ls,ok).
audit(farmer,733,root,'login root',fail).
audit(coleman,736,smith,'login smith',ok).
audit(farmer,747,root,'login root',fail).
audit(farmer,751,root,'login root',ok).
audit(root,760,root,'cd etc',ok).
audit(root,788,etc,'cp passwd ~smith/dont_dare_look_at_this',ok).
audit(smith,819,smith,'emacs tmp1434',344).
audit(root,942,etc,'mail root','Captain Flash strikes again!!!!').
audit(root,947,etc,logout,ok).
audit(smith,1016,smith,'emacs tmp1435',362).
audit(tom,1122,none,'login tom',ok).
audit(tom,1140,tom,'cd ~adams',ok).
audit(tom,1146,adams,'cd ~doe',ok).
audit(tom,1176,doe,ls,ok).
audit(adams,1233,diradams,'emacs auxc',5221).
audit(adams,1237,diradams,logout,ok).
audit(smith,1438,smith,'emacs tmp1436',405).
audit(smith,1444,smith,logout,ok).
audit(tom,1754,doe,'emacs bigpaper',30111).
audit(tom,1759,doe,logout,ok).
audit(doe,2414,none,'login doe',fail).
audit(doe,2421,doe,su,fail).
audit(doe,2421,none,'login doe',ok).
audit(doe,2436,doe,su,fail).
audit(doe,2444,doe,su,fail).
audit(doe,2449,doe,su,ok).
audit(doe,2467,doe,'cd ~adams',ok).
```

```
audit(doe,2473,adams,ls,ok).
audit(doe,2491,adams,'cd ~tom/ba',ok).
audit(doe,2510,ba,'cd ~dog',ok).
audit(doe,2522,dog,ls,ok).
audit(doe,2529,dog,'cd ~adams',ok).
audit(doe,2536,adams,'cd ~tom/ba',ok).
audit(doe,2543,ba,'cd ~root/bin',ok).
audit(doe,2546,bin,'cd ~evans/csclass',ok).
audit(doe,2558,csclass,'cd ~davis',ok).
audit(doe,2569,davis,'cd ~farmer',ok).
audit(doe,2583,farmer,ls,ok).
audit(doe,2596,farmer,'cd ~adams',ok).
audit(doe,2615,adams,'cd ~tom/ba',ok).
audit(doe,2629,ba,'cd bin',ok).
audit(doe,2632,bin,'cd ~evans/csclass',ok).
audit(doe,2636,csclass,'cd ~davis',ok).
audit(doe,2643,davis,'cd ~adams/diradams',ok).
audit(doe,2646,diradams,'cd ~graham',ok).
audit(doe,2670,graham,ls,ok).
audit(doe,2687,adams,'cd ~root',ok).
audit(doe,2687,graham,'cd ~adams',ok).
audit(doe,2709,root,ls,ok).
audit(doe,2720,root,'cd ~adams',ok).
audit(doe,2911,adams,'cat auxa',ok).
audit(doe,2938,adams,'cat auxb',ok).
audit(doe,2979,none,'login doe',fail).
audit(doe,2981,none,'login doe',ok).
audit(doe,2982,doe,su,fail).
audit(doe,2998,doe,su,fail).
audit(doe,3007,doe,su,fail).
audit(doe,3010,doe,su,fail).
audit(doe,3025,doe,su,fail).
audit(doe,3035,doe,su,fail).
audit(doe,3046,doe,su,fail).
audit(doe,3061,doe,su,fail).
audit(doe,3080,doe,su,fail).
audit(doe,3085,doe,su,fail).
audit(doe,3104,doe,su,fail).
audit(doe,3114,doe,su,fail).
audit(doe,3132,adams,'cat auxc',ok).
audit(doe,3133,doe,su,fail).
audit(doe,3152,doe,su,fail).
audit(doe,3163,doe,su,fail).
audit(doe,3174,doe,su,fail).
audit(doe,3186,doe,su,fail).
audit(doe,3187,doe,su,fail).
audit(doe,3195,adams,'cat diradams',ok).
audit(doe,3199,doe,su,fail).
audit(doe,3204,adams,'cd ~tom/ba',ok).
audit(doe,3207,doe,su,fail).
audit(doe,3214,ba,'cd ~graham',ok).
audit(doe,3214,doe,su,fail).
audit(doe,3217,doe,su,fail).
audit(doe,3221,doe,su,fail).
audit(doe,3238,doe,su,fail).
audit(doe,3249,doe,su,fail).
audit(doe,3253,doe,su,fail).
audit(davis,3256,none,'login davis',ok).
audit(doe,3269,doe,su,fail).
audit(doe,3279,doe,su,ok).
audit(doe,3283,doe,'cd ~root/bin',ok).
```

```
audit(doe,3311,bin,ls,ok).
audit(doe,3320,bin,'cd root',ok).
audit(doe,3336,root,ls,ok).
audit(doe,3350,root,'cd ~adams',ok).
audit(doe,3360,adams,'cd ~tom/ba',ok).
audit(doe,3377,ba,'cd ~root/bin',ok).
audit(doe,3379,graham,'cat important',ok).
audit(doe,3390,graham,'cd ~adams',ok).
audit(doe,3403,adams,'cd ~farmer',ok).
audit(davis,3461,davis,'emacs goodnews',1447).
audit(davis,3467,davis,logout,ok).
audit(doe,3512,farmer,'cat secrets',ok).
audit(doe,3516,farmer,logout,ok).
audit(doe,3875,bin,'emacs cd',5038).
audit(doe,4430,bin,'emacs ls',2121).
audit(doe,5140,bin,'emacs please_run_me',22914).
audit(doe,5141,bin,logout,ok).
audit(doe,5147,bin,'login doe',fail).
audit(doe,5155,bin,'login doe',fail).
audit(doe,5169,bin,'login doe',fail).
audit(doe,5176,bin,'login doe',fail).
audit(doe,5186,bin,'login doe',fail).
audit(doe,5192,bin,'login doe',fail).
audit(doe,5193,bin,'login doe',fail).
audit(doe,5203,bin,'login doe',ok).
audit(doe,5204,doe,'cd ~root/bin',ok).
audit(doe,5272,bin,'emacs please_run_me',22914).
audit(doe,5275,bin,logout,ok).
audit(adams,5832,none,'login adams',fail).
audit(adams,5839,none,'login adams',fail).
audit(adams,5846,none,'login adams',ok).
audit(adams,5855,adams,'cd ~root/bin',ok).
audit(adams,5878,bin,ls,fail).
audit(adams,5903,bin,ls,ok).
audit(adams,5915,bin,'cd ~adams',ok).
audit(adams,5920,adams,'cd ~tom/ba',ok).
audit(adams,5935,ba,'cd ~dog',ok).
audit(adams,5957,dog,ls,ok).
audit(adams,5960,dog,'cd ~adams',ok).
audit(adams,5978,adams,'cd ~tom',ok).
audit(adams,6016,tom,ls,fail).
audit(adams,6019,tom,ls,ok).
audit(adams,6036,tom,'cd ~adams',ok).
audit(adams,6052,adams,'cd ~uri',ok).
audit(adams,6086,uri,ls,ok).
audit(adams,6090,uri,'cd ~adams',ok).
audit(adams,6096,adams,'cd ba',ok).
audit(adams,6111,ba,'cd ~root/bin',ok).
audit(adams,6114,bin,'cd ~evans/csclass',ok).
audit(adams,6116,csclass,'cd ~tom',ok).
audit(adams,6138,tom,'rm *',ok).
audit(adams,6297,tom,'mail tom','Haha ful').
audit(adams,6303,tom,logout,ok).
audit(davis,7582,none,'login davis',ok).
audit(smith,7867,none,'login smith',ok).
audit(smith,7872,smith,'cd ~adams',ok).
audit(smith,7891,adams,'cd ~tom',ok).
audit(davis,8012,davis,'emacs topsecret',1572).
audit(davis,8013,davis,logout,ok).
audit(smith,8027,tom,'emacs bb',451).
audit(smith,8029,tom,'mail root',bad(cd,bin)).
```

```
audit(smith,8036,tom,logout,ok).
audit(root,8573,none,'login root',ok).
audit(root,8586,root,'cd ~adams',ok).
audit(root,8604,adams,'cd ~root/bin',ok).
audit(root,8642,bin,ls,ok).
audit(root,8645,bin,'mail root',bad(cd,bin)).
audit(root,8654,bin,'cd ~adams',ok).
audit(root,8667,adams,'cd ~tom/ba',ok).
audit(root,8684,ba,'cd ~root/bin',ok).
audit(root,8696,bin,'cd ~graham',ok).
audit(root,8730,graham,ls,ok).
audit(root,8826,graham,'login graham',ok).
audit(graham,9382,graham,'emacs important',10219).
audit(graham,9390,graham,logout,ok).
audit(graham,9994,none,'login graham',ok).
audit(graham,9997,graham,'cd ~tom',ok).
audit(graham,10033,tom,ls,ok).
audit(graham,10037,tom,'emacs aa',658).
audit(graham,10044,tom,logout,ok).
```

The following is the script of Run 2:

```
Script started on Wed Mar 15 22:33:52 1995
.alias: No such file or directory.
ai2:/users/work4/schiavo/Thesis/Tutor>>prolog


Quintus Prolog Release 3.1.1 (Sun-4, SunOS 4.0)
Copyright (C) 1990, Quintus Corporation.  All rights reserved.
2100 Geng Road, Palo Alto, California U.S.A. (415) 813-3800

| ?- [intruder].
% compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/intruder.pl
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/metutor30.pl
% Undefined procedures will just fail ('fail' option)
%    loading file /usr/local/q3.1.1/generic/qplib3.1.1/library/random.qof
%     foreign file /usr/local/q3.1.1/generic/qplib3.1.1/library/sun4-4/libpl.so loaded
%    random.qof loaded, 0.100 sec 9,392 bytes
%    module random imported into user
* Clauses for writefact/2 are not together in the source file
%  metutor30.pl compiled in module user, 3.016 sec 50,420 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/modrowe5
%  modrowe5 compiled in module user, 0.633 sec 14,724 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/filetree
%  filetree compiled in module user, 0.433 sec 5,296 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/rules
* Clauses for behavior/5 are not together in the source file
* Clauses for behavior/4 are not together in the source file
%  rules compiled in module user, 0.616 sec 7,440 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/rowefiles
%  rowefiles compiled in module user, 0.100 sec 4,252 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/operators
* Clauses for recommended/3 are not together in the source file
* Clauses for recommended/2 are not together in the source file
* Clauses for addpostcondition/2 are not together in the source file
%  operators compiled in module user, 0.600 sec 8,308 bytes
% intruder.pl compiled in module user, 6.283 sec 101,320 bytes
```

```
yes
| ?- statistics.

memory (total)          649696 bytes:     464956 in use,     184740 free
   program space        333892 bytes
   global space          65532 bytes:      26688 in use,      38844 free
      global stack                         24584 bytes
      trail                                   16 bytes
      system                                2088 bytes
   local stack           65532 bytes:        440 in use,      65092 free
      local stack                           416 bytes
      system                                 24 bytes

 0.000 sec. for 0 global and 3 local space shifts
 0.000 sec. for 0 garbage collections which collected 0 bytes
 6.566 sec. runtime

yes
| ?- start.

*******************************************************************************
*                                                                             *
*                                  AUDIT FILE                                 *
*                                                                             *
*      The following displays the current contents of the audit file:         *
*                                                                             *
*******************************************************************************


Name       Time     Path           Command       Result

adams       122     adams            cd ~adams     ok
adams       125     adams          cd diradams     ok
adams       500     diradams        emacs auxb     1229
adams      1233     diradams        emacs auxc     5221
adams      1237     diradams            logout     ok
adams      5832     none           login adams     fail
adams      5839     none           login adams     fail
adams      5846     none           login adams     ok
adams      5855     adams        cd ~root/bin      ok
adams      5878     bin                    ls      fail
adams      5903     bin                    ls      ok
adams      5915     bin              cd ~adams     ok
adams      5920     adams           cd ~tom/ba     ok
adams      5935     ba                 cd ~dog     ok
adams      5957     dog                    ls      ok
adams      5960     dog              cd ~adams     ok
adams      5978     adams              cd ~tom     ok
adams      6016     tom                    ls      fail
adams      6019     tom                    ls      ok
adams      6036     tom              cd ~adams     ok
adams      6052     adams              cd ~uri     ok
adams      6086     uri                    ls      ok
adams      6090     uri              cd ~adams     ok
adams      6096     adams               cd ba      ok
adams      6111     ba           cd ~root/bin      ok
adams      6114     bin     cd ~evans/csclass      ok
adams      6116     csclass            cd ~tom     ok
adams      6138     tom                  rm *      ok
adams      6297     tom              mail tom      Haha ful
adams      6303     tom                logout      ok
```

coleman	622	none	login coleman	fail
coleman	632	none	login coleman	fail
coleman	636	none	login coleman	ok
coleman	652	coleman	cd ~smith	ok
coleman	684	smith	ls	ok
coleman	729	smith	ls	ok
coleman	736	smith	login smith	ok
davis	9	none	login davis	ok
davis	14	davis	cd ~adams	ok
davis	21	adams	ls	ok
davis	96	adams	login adams	fail
davis	108	adams	login adams	ok
davis	3256	none	login davis	ok
davis	3461	davis	emacs goodnews	1447
davis	3467	davis	logout	ok
davis	7582	none	login davis	ok
davis	8012	davis	emacs topsecret	1572
davis	8013	davis	logout	ok
doe	2414	none	login doe	fail
doe	2421	doe	su	fail
doe	2421	none	login doe	ok
doe	2436	doe	su	fail
doe	2444	doe	su	fail
doe	2449	doe	su	ok
doe	2467	doe	cd ~adams	ok
doe	2473	adams	ls	ok
doe	2491	adams	cd ~tom/ba	ok
doe	2510	ba	cd ~dog	ok
doe	2522	dog	ls	ok
doe	2529	dog	cd ~adams	ok
doe	2536	adams	cd ~tom/ba	ok
doe	2543	ba	cd ~root/bin	ok
doe	2546	bin	cd ~evans/csclass	ok
doe	2558	csclass	cd ~davis	ok
doe	2569	davis	cd ~farmer	ok
doe	2583	farmer	ls	ok
doe	2596	farmer	cd ~adams	ok
doe	2615	adams	cd ~tom/ba	ok
doe	2629	ba	cd bin	ok
doe	2632	bin	cd ~evans/csclass	ok
doe	2636	csclass	cd ~davis	ok
doe	2643	davis	cd ~adams/diradams	ok
doe	2646	diradams	cd ~graham	ok
doe	2670	graham	ls	ok
doe	2687	adams	cd ~root	ok
doe	2687	graham	cd ~adams	ok
doe	2709	root	ls	ok
doe	2720	root	cd ~adams	ok
doe	2911	adams	cat auxa	ok
doe	2938	adams	cat auxb	ok
doe	2979	none	login doe	fail
doe	2981	none	login doe	ok
doe	2982	doe	su	fail
doe	2998	doe	su	fail
doe	3007	doe	su	fail
doe	3010	doe	su	fail
doe	3025	doe	su	fail
doe	3035	doe	su	fail
doe	3046	doe	su	fail
doe	3061	doe	su	fail
doe	3080	doe	su	fail

```
doe         3085     doe                    su      fail
doe         3104     doe                    su      fail
doe         3114     doe                    su      fail
doe         3132     adams           cat auxc       ok
doe         3133     doe                    su      fail
doe         3152     doe                    su      fail
doe         3163     doe                    su      fail
doe         3174     doe                    su      fail
doe         3186     doe                    su      fail
doe         3187     doe                    su      fail
doe         3195     adams        cat diradams      ok
doe         3199     doe                    su      fail
doe         3204     adams          cd ~tom/ba      ok
doe         3207     doe                    su      fail
doe         3214     ba             cd ~graham      ok
doe         3214     doe                    su      fail
doe         3217     doe                    su      fail
doe         3221     doe                    su      fail
doe         3238     doe                    su      fail
doe         3249     doe                    su      fail
doe         3253     doe                    su      fail
doe         3269     doe                    su      fail
doe         3279     doe                    su      ok
doe         3283     doe          cd ~root/bin      ok
doe         3311     bin                    ls      ok
doe         3320     bin              cd root       ok
doe         3336     root                   ls      ok
doe         3350     root           cd ~adams       ok
doe         3360     adams          cd ~tom/ba      ok
doe         3377     ba           cd ~root/bin      ok
doe         3379     graham      cat important      ok
doe         3390     graham         cd ~adams       ok
doe         3403     adams          cd ~farmer      ok
doe         3512     farmer       cat secrets       ok
doe         3516     farmer             logout      ok
doe         3875     bin              emacs cd      5038
doe         4430     bin              emacs ls      2121
doe         5140     bin   emacs please_run_me      22914
doe         5141     bin                logout      ok
doe         5147     bin             login doe      fail
doe         5155     bin             login doe      fail
doe         5169     bin             login doe      fail
doe         5176     bin             login doe      fail
doe         5186     bin             login doe      fail
doe         5192     bin             login doe      fail
doe         5193     bin             login doe      fail
doe         5203     bin             login doe      ok
doe         5204     doe          cd ~root/bin      ok
doe         5272     bin   emacs please_run_me      22914
doe         5275     bin                logout      ok
evans        340     none          login evans      ok
evans        625     evans       emacs csclass      511
evans        655     evans           mail root      bad(csclass,evans)
evans        657     evans             logout       ok
farmer       668     farmer       cd ~root/bin      ok
farmer       668     none         login farmer      ok
farmer       671     bin                    ls      ok
farmer       687     bin              cd ~root      ok
farmer       707     root                   ls      ok
farmer       711     root           login root      fail
farmer       716     root           login root      fail
```

```
farmer      720     root           login root     fail
farmer      722     root           login root     fail
farmer      733     root           login root     fail
farmer      747     root           login root     fail
farmer      751     root           login root     ok
graham     9382     graham    emacs important     10219
graham     9390     graham             logout     ok
graham     9994     none         login graham     ok
graham     9997     graham            cd ~tom     ok
graham    10033     tom                    ls     ok
graham    10037     tom              emacs aa     658
graham    10044     tom                logout     ok
root        760     root               cd etc     ok
root        788     etccp passwd ~smith/dont_dare_look_at_this     ok
root        942     etc              mail root     Captain Flash strikes again!!!!
root        947     etc                logout     ok
root       8573     none             login root     ok
root       8586     root              cd ~adams     ok
root       8604     adams         cd ~root/bin     ok
root       8642     bin                    ls     ok
root       8645     bin              mail root     bad(cd,bin)
root       8654     bin              cd ~adams     ok
root       8667     adams           cd ~tom/ba     ok
root       8684     ba             cd ~root/bin     ok
root       8696     bin              cd ~graham     ok
root       8730     graham                 ls     ok
root       8826     graham       login graham     ok
smith       819     smith        emacs tmp1434     344
smith      1016     smith        emacs tmp1435     362
smith      1438     smith        emacs tmp1436     405
smith      1444     smith               logout     ok
smith      7867     none           login smith     ok
smith      7872     smith            cd ~adams     ok
smith      7891     adams              cd ~tom     ok
smith      8027     tom               emacs bb     451
smith      8029     tom              mail root     bad(cd,bin)
smith      8036     tom                 logout     ok
tom        1122     none             login tom     ok
tom        1140     tom              cd ~adams     ok
tom        1146     adams              cd ~doe     ok
tom        1176     doe                    ls     ok
tom        1754     doe         emacs bigpaper     30111
tom        1759     doe                 logout     ok
```

```
*****************************************************************************
*                                                                           *
*                                MAIL RECEIVED                              *
*                                                                           *
*      The following displays mail received by root:                        *
*                                                                           *
*****************************************************************************
```

```
From        To      Time        Problem(File,Directory)

evans       root    655         bad(csclass,evans)
root        root    942         Captain Flash strikes again!!!!
root        root    8645        bad(cd,bin)
smith       root    8029        bad(cd,bin)
```

```
% Undefined procedures will just fail ('fail' option)
Warnings:
This fact is not removable: changed(password,root)
This fact is not removable: confronted(user,_12829)
This fact is not removable: examined(password,_12763)
This fact is not removable: executed(password,cracker)
This fact is not removable: investigated(password,_12742)
This fact is not removable: changed(password,for,_12700)
This fact is not removable: changed(permissions,file,_12872)
This fact is not removable: restored(password,for,_12808)
This fact is not removable: issued(new,password,to,_12786)

Your objectives:
backup tape is stored and password cracker is executed.
Wait a moment while I analyze the problem thoroughly.

*************************************************************************
*                                                                       *
*  To see a list of possible actions, type the letter "h" or the word   *
*  "help." To review the audit file or your mail at anytime, type the   *
*  word "auditfile" or "mail" respectively.                             *
*                                                                       *
*************************************************************************
Type h for help.
************ These facts are now true: *************
backup tape is stored,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
and mail(smith,root,8029,bad(cd,bin)) is true.
Select an action: execute password cracker
You chose to execute password cracker.
OK, but a hint: "change permissions file passwd"
 is more important now than "execute password cracker".
************ These facts are now true: *************
password cracker is executed,
backup tape is stored,
known(insecure,password,for,_201271) is true,
known(insecure,password,for,_201278) is true,
known(insecure,password,for,_201285) is true,
known(insecure,password,for,_201292) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
and mail(smith,root,8029,bad(cd,bin)) is true.
Select an action: change permissions file passwd
You chose to change permissions file passwd.
>>>>Operator change(permissions,file,passwd) could not be applied to:
password cracker is executed,
backup tape is stored,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
and mail(smith,root,8029,bad(cd,bin)) is true
>>>>Operator change(permissions,file,passwd) could not be applied to:
password cracker is executed,
backup tape is stored,
```

```
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
and mail(smith,root,8029,bad(cd,bin)) is true
Have you confused that with the check permissions file passwd action?
That action requires that:
checked(permissions,file,passwd) is true.
************ These facts are now true: *************
password cracker is executed,
backup tape is stored,
known(insecure,password,for,_208775) is true,
known(insecure,password,for,_208782) is true,
known(insecure,password,for,_208789) is true,
known(insecure,password,for,_208796) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
and mail(smith,root,8029,bad(cd,bin)) is true.
Select an action: check permissions file passwd
You chose to check permissions file passwd.
OK.
************ These facts are now true: *************
password cracker is executed,
backup tape is stored,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
and mail(smith,root,8029,bad(cd,bin)) is true.
Select an action: change permissions file passwd
You chose to change permissions file passwd.
OK.
************ These facts are now true: *************
password cracker is executed,
backup tape is stored,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
and mail(smith,root,8029,bad(cd,bin)) is true.
Select an action: change password for adams
You chose to change password for adams.
OK, but a hint: "change root password"
 is more important now than "change password for adams".
************ These facts are now true: *************
password cracker is executed,
backup tape is stored,
changed(password,for,adams) is true,
```

```
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
and mail(smith,root,8029,bad(cd,bin)) is true.
Select an action: change root password
You chose to change root password.
OK.
************ These facts are now true: *************
password root is changed,
password cracker is executed,
backup tape is stored,
changed(password,for,adams) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
and mail(smith,root,8029,bad(cd,bin)) is true.
Select an action: change password for farmer
You chose to change password for farmer.
OK, but a hint: "compare file cd for Trojan Horse with cd on backup tape"
 is more important now than "change password for farmer".
************ These facts are now true: *************
password root is changed,
password cracker is executed,
backup tape is stored,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
and mail(smith,root,8029,bad(cd,bin)) is true.
Select an action: loacte backup tape
You chose to loacte backup tape.
I assume you mean locate backup tape.
OK.
************ These facts are now true: *************
password root is changed,
password cracker is executed,
backup tape is located,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
```

```
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
and mail(smith,root,8029,bad(cd,bin)) is true.
Select an action: load backup tape
You chose to load backup tape.
OK.
************ These facts are now true: *************
password root is changed,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
and mail(smith,root,8029,bad(cd,bin)) is true.
Select an action: find file cd on backup tape
You chose to find file cd on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
mail(smith,root,8029,bad(cd,bin)) is true,
and found(file,cd,on,backup,tape) is true.
Select an action: compare file cd for Trojan Horse with cd on backup tape
You chose to compare file cd for Trojan Horse with cd on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
```

```
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
mail(smith,root,8029,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
and compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true.
Select an action: find file ls on backup tape
You chose to find file ls on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
mail(smith,root,8029,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
and compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true.
Select an action: compare file ls for Trojan Horse with ls on backup tape
You chose to compare file ls for Trojan Horse with ls on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
mail(smith,root,8029,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: change password for graham
You chose to change password for graham.
OK, but a hint: "confront user doe"
 is more important now than "change password for graham".
************ These facts are now true: *************
```

```
password root is changed,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(password,for,graham) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
mail(smith,root,8029,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: confront user doe
You chose to confront user doe.
OK.
************ These facts are now true: *************
password root is changed,
user doe is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(password,for,graham) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
mail(smith,root,8029,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: change password for smith
You chose to change password for smith.
OK, but a hint: "restore modified file cd from backup"
 is more important now than "change password for smith".
************ These facts are now true: *************
password root is changed,
user doe is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(password,for,graham) is true,
changed(password,for,smith) is true,
```

```
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
mail(smith,root,8029,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore modified file cd from backup
You chose to restore modified file cd from backup.
OK.
************ These facts are now true: *************
password root is changed,
user doe is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file cd is restored,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(password,for,graham) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
mail(smith,root,8029,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: h
Possible actions are:
change root password,
confront user _498410,
execute password cracker,
load backup tape,
locate backup tape,
store backup tape,
change password for _498436,
change permissions file passwd,
check permissions file _498448,
examine user password _498454,
investigate user password _498460,
issue _498464 new user password,
remove Trojan Horse from _498474,
restore user password for _498481,
find file _498486 on backup tape,
restore deleted file _498495 from backup,
restore modified file _498503 from backup,
```

```
restore modified file passwd from backup,
and compare file _498518 for Trojan Horse with _498518 on backup tape.
Possible commands to the tutor are:
help,
exit,
auditfile,
and mail.
Your objectives are:
password cracker must be executed and backup tape must be stored.
************ These facts are now true: *************
password root is changed,
user doe is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file cd is restored,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(password,for,graham) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
mail(smith,root,8029,bad(cd,bin)) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: find file bb on backup tape
You chose to find file bb on backup tape.
Have you confused that with the find file aa on backup tape action?
OK, but a hint: "restore deleted file aa from backup"
 is more important now than "restore deleted file bb from backup".
************ These facts are now true: *************
password root is changed,
user doe is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file cd is restored,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(password,for,graham) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
mail(smith,root,8029,bad(cd,bin)) is true,
found(file,bb,on,backup,tape) is true,
```

```
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: find file aa on backup tape
You chose to find file aa on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user doe is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file cd is restored,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(password,for,graham) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
mail(smith,root,8029,bad(cd,bin)) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore deleted file aa from backup
You chose to restore deleted file aa from backup.
OK.
************ These facts are now true: *************
password root is changed,
user doe is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file aa is restored,
file cd is restored,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(password,for,graham) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
mail(smith,root,8029,bad(cd,bin)) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
```

```
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore deleted file bb from backup
You chose to restore deleted file bb from backup.
OK.
************ These facts are now true: *************
password root is changed,
user doe is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file aa is restored,
file bb is restored,
file cd is restored,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(password,for,graham) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(evans,root,655,bad(csclass,evans)) is true,
mail(root,root,942,Captain Flash strikes again!!!!) is true,
mail(root,root,8645,bad(cd,bin)) is true,
mail(smith,root,8029,bad(cd,bin)) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: store backup tape
You chose to store backup tape.
OK.
Congratulations! You have done the job.
The session is over.  Do "go." to restart.

yes
| ?- statistics.

memory (total)          2353632 bytes:    1305836 in use,    1047796 free
   program space        1174772 bytes
   global space           65532 bytes:      26820 in use,      38712 free
      global stack                          24692 bytes
      trail                                    40 bytes
      system                                 2088 bytes
   local stack            65532 bytes:        648 in use,      64884 free
      local stack                           624 bytes
      system                                 24 bytes

 0.000 sec. for 0 global and 32 local space shifts
 0.233 sec. for 1 garbage collections which collected 1017792 bytes
 47.100 sec. runtime

yes
| ?- halt.
```

TAB 3. RUN 3

The following is the audit file used for Run 3:

```
audit(jones,1680,none,'login jones',ok).
audit(jones,1681,jones,'cd ~smith',ok).
audit(jones,1716,smith,ls,ok).
audit(jones,1818,smith,'login smith',ok).
audit(smith,2368,smith,'emacs tmp1434',344).
audit(smith,3000,smith,'emacs tmp1435',362).
audit(evans,3287,none,'login evans',ok).
audit(evans,3303,evans,'cd ~root/bin',ok).
audit(evans,3331,bin,ls,ok).
audit(evans,3440,bin,'cd ~adams',ok).
audit(evans,3452,adams,'cd ~graham',ok).
audit(smith,3465,smith,'emacs tmp1436',405).
audit(evans,3469,graham,ls,ok).
audit(smith,3473,smith,logout,ok).
audit(uri,3550,none,'login uri',ok).
audit(uri,3561,uri,'cd ~adams',ok).
audit(uri,3569,adams,'cd ~root/bin',ok).
audit(uri,3602,bin,ls,ok).
audit(uri,3609,bin,'cd ~adams',ok).
audit(uri,3626,adams,'cd ~root',ok).
audit(evans,3627,graham,'login graham',ok).
audit(uri,3634,root,ls,fail).
audit(uri,3646,root,ls,fail).
audit(uri,3677,root,ls,fail).
audit(uri,3680,root,ls,ok).
audit(uri,3691,root,'login root',fail).
audit(uri,3699,root,'login root',fail).
audit(uri,3704,root,'login root',fail).
audit(uri,3705,root,'login root',fail).
audit(uri,3708,root,'login root',fail).
audit(uri,3722,root,'login root',fail).
audit(uri,3735,root,'login root',ok).
audit(root,3755,root,'cd etc',ok).
audit(root,3796,etc,'cp passwd ~smith/dont_dare_look_at_this',ok).
audit(dog,3890,none,'login dog',fail).
audit(dog,3897,none,'login dog',fail).
audit(dog,3900,none,'login dog',fail).
audit(dog,3908,none,'login dog',fail).
audit(dog,3918,none,'login dog',fail).
audit(dog,3924,none,'login dog',fail).
audit(dog,3934,none,'login dog',fail).
audit(dog,3940,none,'login dog',ok).
audit(dog,3941,dog,su,fail).
audit(dog,3948,dog,su,fail).
audit(farmer,3954,none,'login farmer',fail).
audit(dog,3955,dog,su,fail).
audit(dog,3958,dog,su,fail).
audit(farmer,3966,none,'login farmer',fail).
audit(dog,3971,dog,su,fail).
audit(farmer,3974,none,'login farmer',fail).
audit(root,3974,etc,'mail root','Captain Flash strikes again!!!!').
audit(root,3978,etc,logout,ok).
audit(dog,3985,dog,su,fail).
audit(farmer,3985,none,'login farmer',ok).
```

```
audit(farmer,3990,farmer,su,fail).
audit(dog,3994,dog,su,fail).
audit(dog,3995,dog,su,fail).
audit(farmer,3996,farmer,su,fail).
audit(dog,4014,dog,su,fail).
audit(farmer,4015,farmer,su,fail).
audit(farmer,4026,farmer,su,fail).
audit(farmer,4028,farmer,su,fail).
audit(farmer,4032,farmer,su,fail).
audit(dog,4034,dog,su,fail).
audit(farmer,4039,farmer,su,fail).
audit(dog,4047,dog,su,fail).
audit(farmer,4056,farmer,su,ok).
audit(farmer,4057,farmer,'cd ~adams',ok).
audit(dog,4060,dog,su,fail).
audit(farmer,4064,adams,ls,ok).
audit(dog,4077,dog,su,fail).
audit(dog,4082,dog,su,fail).
audit(farmer,4083,adams,'cd ~dog',ok).
audit(dog,4093,dog,su,fail).
audit(graham,4098,graham,'emacs important',10444).
audit(graham,4099,graham,logout,ok).
audit(farmer,4105,dog,ls,ok).
audit(dog,4108,dog,su,fail).
audit(dog,4119,dog,su,fail).
audit(farmer,4123,dog,'cd ~adams',ok).
audit(dog,4133,dog,su,fail).
audit(farmer,4137,adams,'cd ~tom/ba',ok).
audit(farmer,4144,ba,'cd ~farmer',ok).
audit(dog,4150,dog,su,fail).
audit(farmer,4152,farmer,ls,fail).
audit(dog,4166,dog,su,fail).
audit(dog,4170,dog,su,fail).
audit(dog,4182,dog,su,fail).
audit(farmer,4184,farmer,ls,ok).
audit(dog,4186,dog,su,fail).
audit(dog,4187,dog,su,fail).
audit(farmer,4195,farmer,'cd ~graham',ok).
audit(dog,4202,dog,su,fail).
audit(farmer,4210,graham,ls,ok).
audit(davis,4213,none,'login davis',ok).
audit(dog,4214,dog,su,fail).
audit(farmer,4217,graham,'cd ~root',ok).
audit(dog,4220,dog,su,fail).
audit(dog,4230,dog,su,fail).
audit(farmer,4232,root,ls,ok).
audit(farmer,4234,root,'cd ~adams',ok).
audit(dog,4242,dog,su,fail).
audit(farmer,4252,adams,'cat auxa',ok).
audit(dog,4258,dog,su,fail).
audit(dog,4260,dog,su,ok).
audit(dog,4271,dog,'cd ~root/bin',ok).
audit(dog,4287,bin,ls,fail).
audit(dog,4310,bin,ls,ok).
audit(dog,4330,bin,'cd ~root',ok).
audit(dog,4354,root,ls,ok).
audit(dog,4367,root,'cd ~adams',ok).
audit(dog,4381,adams,'cd ~root/bin',ok).
audit(farmer,4412,adams,'cat auxb',ok).
audit(davis,4490,davis,'emacs goodnews',1258).
audit(davis,4490,davis,logout,ok).
```

```
audit(farmer,4494,adams,'cat auxc',ok).
audit(dog,4558,dog,'cd ~tom',ok).
audit(dog,4558,none,'login dog',ok).
audit(farmer,4710,adams,'cat diradams',ok).
audit(farmer,4719,adams,'cd ~tom/ba',ok).
audit(farmer,4720,ba,'cd ~root/bin',ok).
audit(farmer,4738,bin,'cd ~graham',ok).
audit(dog,4766,tom,'emacs bb',540).
audit(farmer,4836,graham,'cat important',ok).
audit(farmer,4849,graham,'cd ~farmer',ok).
audit(dog,4895,bin,'emacs cd',5075).
audit(dog,4906,tom,'mail root',bad(bb,tom)).
audit(dog,4909,tom,logout,ok).
audit(farmer,5002,farmer,'cat secrets',ok).
audit(farmer,5005,farmer,logout,ok).
audit(root,5006,none,'login root',fail).
audit(root,5010,none,'login root',fail).
audit(root,5014,none,'login root',fail).
audit(root,5016,none,'login root',fail).
audit(root,5021,none,'login root',fail).
audit(root,5030,none,'login root',ok).
audit(root,5045,root,'cd ~root/bin',ok).
audit(root,5051,bin,ls,fail).
audit(root,5071,bin,ls,ok).
audit(root,5079,bin,'cd ~adams',ok).
audit(root,5094,adams,'cd ~tom/ba',ok).
audit(root,5096,ba,'cd ~evans/csclass',ok).
audit(root,5108,csclass,'cd ~davis',ok).
audit(root,5128,davis,'cd ~adams/diradams',ok).
audit(root,5143,diradams,'cd ~doe',ok).
audit(root,5147,doe,'cd ~dog',ok).
audit(root,5186,dog,ls,fail).
audit(root,5214,dog,ls,fail).
audit(root,5246,dog,ls,ok).
audit(root,5249,dog,'cd ~adams',ok).
audit(root,5257,adams,'cd ~tom/ba',ok).
audit(brown,5271,none,'login brown',ok).
audit(brown,5275,brown,'cd ~adams',ok).
audit(root,5275,ba,'cd ~tom',ok).
audit(root,5276,tom,ls,ok).
audit(root,5284,tom,'cd ~adams',ok).
audit(dog,5289,bin,'emacs ls',2120).
audit(root,5294,adams,'cd ~tom/ba',ok).
audit(root,5310,ba,'cd ~root/bin',ok).
audit(root,5311,bin,'cd ~evans/csclass',ok).
audit(brown,5313,adams,ls,ok).
audit(root,5322,csclass,'cd ~uri',ok).
audit(root,5335,uri,ls,ok).
audit(root,5344,uri,'cd ~adams',ok).
audit(root,5355,adams,'cd ~tom/ba',ok).
audit(jones,5359,none,'login jones',ok).
audit(root,5371,ba,'cd ~root/bin',ok).
audit(root,5374,bin,'cd ~tom',ok).
audit(jones,5377,jones,'cd ~doe',ok).
audit(jones,5386,doe,ls,ok).
audit(root,5394,tom,'rm *',ok).
audit(root,5417,tom,'mail tom','Haha ful').
audit(root,5419,tom,logout,ok).
audit(jones,5435,doe,'mail root',bad(cd,bin)).
audit(brown,5455,adams,'mail root',bad(cd,bin)).
audit(brown,5456,adams,'login adams',ok).
```

```
audit(adams,5469,adams,'cd diradams',ok).
audit(adams,5669,diradams,'emacs auxb',1354).
audit(adams,5709,diradams,'mail root',bad(cd,bin)).
audit(jones,5798,doe,'emacs bigpaper',29935).
audit(jones,5798,doe,logout,ok).
audit(davis,5941,none,'login davis',fail).
audit(davis,5941,none,'login davis',ok).
audit(davis,5963,davis,'emacs topsecret',1572).
audit(davis,5970,davis,logout,ok).
audit(dog,6085,bin,'emacs please_run_me',22914).
audit(dog,6088,bin,logout,ok).
audit(dog,6099,bin,'login dog',fail).
audit(dog,6101,bin,'login dog',fail).
audit(dog,6103,bin,'login dog',fail).
audit(dog,6110,bin,'login dog',fail).
audit(dog,6112,bin,'login dog',fail).
audit(dog,6113,bin,'login dog',fail).
audit(dog,6125,bin,'login dog',fail).
audit(dog,6128,bin,'login dog',fail).
audit(dog,6139,bin,'login dog',fail).
audit(dog,6153,bin,'login dog',fail).
audit(dog,6160,bin,'login dog',fail).
audit(dog,6172,bin,'login dog',fail).
audit(dog,6173,bin,'login dog',fail).
audit(dog,6184,bin,'login dog',fail).
audit(dog,6196,bin,'login dog',fail).
audit(dog,6199,bin,'login dog',ok).
audit(dog,6216,dog,'cd ~adams',ok).
audit(dog,6234,adams,'cd ~tom/ba',ok).
audit(dog,6237,ba,'cd ~root/bin',ok).
audit(adams,6266,diradams,'emacs auxc',5060).
audit(adams,6268,diradams,logout,ok).
audit(dog,6397,bin,'emacs please_run_me',22914).
audit(dog,6403,bin,logout,ok).
audit(evans,6867,none,'login evans',ok).
audit(evans,6956,evans,'emacs csclass',519).
audit(evans,6962,evans,logout,ok).
audit(graham,8088,none,'login graham',ok).
audit(graham,8098,graham,'cd ~tom',ok).
audit(graham,8121,tom,ls,ok).
audit(graham,8266,tom,'mail root',bad(cd,bin)).
audit(graham,8855,tom,'emacs aa',549).
audit(graham,8858,tom,logout,ok).
```

The following is the script of Run 3:

```
Script started on Wed Mar 15 22:45:04 1995
.alias: No such file or directory.
[7mai2:/users/work4/schiavo/Thesis/Tutor>>[mprolog


Quintus Prolog Release 3.1.1 (Sun-4, SunOS 4.0)
Copyright (C) 1990, Quintus Corporation.  All rights reserved.
2100 Geng Road, Palo Alto, California U.S.A. (415) 813-3800

| ?- [intruder].
% compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/intruder.pl
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/metutor30.pl
% Undefined procedures will just fail ('fail' option)
```

```
%   loading file /usr/local/q3.1.1/generic/qplib3.1.1/library/random.qof
%    foreign file /usr/local/q3.1.1/generic/qplib3.1.1/library/sun4-4/libpl.so loaded
%   random.qof loaded, 0.117 sec 9,392 bytes
%   module random imported into user
* Clauses for writefact/2 are not together in the source file
%  metutor30.pl compiled in module user, 3.150 sec 50,420 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/modrowe6
%  modrowe6 compiled in module user, 0.733 sec 16,388 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/filetree
%  filetree compiled in module user, 0.433 sec 5,296 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/rules
* Clauses for behavior/5 are not together in the source file
* Clauses for behavior/4 are not together in the source file
%  rules compiled in module user, 0.633 sec 7,440 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/rowefiles
%  rowefiles compiled in module user, 0.100 sec 4,304 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/operators
* Clauses for recommended/3 are not together in the source file
* Clauses for recommended/2 are not together in the source file
* Clauses for addpostcondition/2 are not together in the source file
%  operators compiled in module user, 0.584 sec 8,348 bytes
% intruder.pl compiled in module user, 6.383 sec 103,092 bytes

yes
| ?- statistics.

memory (total)          649696 bytes:     466728 in use,     182968 free
   program space        335664 bytes
   global space          65532 bytes:      26688 in use,      38844 free
      global stack                         24584 bytes
      trail                                   16 bytes
      system                                2088 bytes
   local stack           65532 bytes:        440 in use,      65092 free
      local stack                           416 bytes
      system                                 24 bytes

 0.017 sec. for 0 global and 3 local space shifts
 0.000 sec. for 0 garbage collections which collected 0 bytes
 6.733 sec. runtime

yes
| ?- start.

*********************************************************************************
*                                                                               *
*                                  AUDIT FILE                                   *
*                                                                               *
*      The following displays the current contents of the audit file:           *
*                                                                               *
*********************************************************************************


Name        Time      Path           Command        Result

adams       5469      adams          cd diradams     ok
adams       5669      diradams        emacs auxb     1354
adams       5709      diradams         mail root     bad(cd,bin)
adams       6266      diradams        emacs auxc     5060
adams       6268      diradams            logout     ok
brown       5271      none           login brown     ok
brown       5275      brown            cd ~adams     ok
```

brown	5313	adams	ls	ok
brown	5455	adams	mail root	bad(cd,bin)
brown	5456	adams	login adams	ok
davis	4213	none	login davis	ok
davis	4490	davis	emacs goodnews	1258
davis	4490	davis	logout	ok
davis	5941	none	login davis	fail
davis	5941	none	login davis	ok
davis	5963	davis	emacs topsecret	1572
davis	5970	davis	logout	ok
dog	3890	none	login dog	fail
dog	3897	none	login dog	fail
dog	3900	none	login dog	fail
dog	3908	none	login dog	fail
dog	3918	none	login dog	fail
dog	3924	none	login dog	fail
dog	3934	none	login dog	fail
dog	3940	none	login dog	ok
dog	3941	dog	su	fail
dog	3948	dog	su	fail
dog	3955	dog	su	fail
dog	3958	dog	su	fail
dog	3971	dog	su	fail
dog	3985	dog	su	fail
dog	3994	dog	su	fail
dog	3995	dog	su	fail
dog	4014	dog	su	fail
dog	4034	dog	su	fail
dog	4047	dog	su	fail
dog	4060	dog	su	fail
dog	4077	dog	su	fail
dog	4082	dog	su	fail
dog	4093	dog	su	fail
dog	4108	dog	su	fail
dog	4119	dog	su	fail
dog	4133	dog	su	fail
dog	4150	dog	su	fail
dog	4166	dog	su	fail
dog	4170	dog	su	fail
dog	4182	dog	su	fail
dog	4186	dog	su	fail
dog	4187	dog	su	fail
dog	4202	dog	su	fail
dog	4214	dog	su	fail
dog	4220	dog	su	fail
dog	4230	dog	su	fail
dog	4242	dog	su	fail
dog	4258	dog	su	fail
dog	4260	dog	su	ok
dog	4271	dog	cd ~root/bin	ok
dog	4287	bin	ls	fail
dog	4310	bin	ls	ok
dog	4330	bin	cd ~root	ok
dog	4354	root	ls	ok
dog	4367	root	cd ~adams	ok
dog	4381	adams	cd ~root/bin	ok
dog	4558	dog	cd ~tom	ok
dog	4558	none	login dog	ok
dog	4766	tom	emacs bb	540
dog	4895	bin	emacs cd	5075
dog	4906	tom	mail root	bad(bb,tom)

dog	4909	tom	logout	ok
dog	5289	bin	emacs ls	2120
dog	6085	bin	emacs please_run_me	22914
dog	6088	bin	logout	ok
dog	6099	bin	login dog	fail
dog	6101	bin	login dog	fail
dog	6103	bin	login dog	fail
dog	6110	bin	login dog	fail
dog	6112	bin	login dog	fail
dog	6113	bin	login dog	fail
dog	6125	bin	login dog	fail
dog	6128	bin	login dog	fail
dog	6139	bin	login dog	fail
dog	6153	bin	login dog	fail
dog	6160	bin	login dog	fail
dog	6172	bin	login dog	fail
dog	6173	bin	login dog	fail
dog	6184	bin	login dog	fail
dog	6196	bin	login dog	fail
dog	6199	bin	login dog	ok
dog	6216	dog	cd ~adams	ok
dog	6234	adams	cd ~tom/ba	ok
dog	6237	ba	cd ~root/bin	ok
dog	6397	bin	emacs please_run_me	22914
dog	6403	bin	logout	ok
evans	3287	none	login evans	ok
evans	3303	evans	cd ~root/bin	ok
evans	3331	bin	ls	ok
evans	3440	bin	cd ~adams	ok
evans	3452	adams	cd ~graham	ok
evans	3469	graham	ls	ok
evans	3627	graham	login graham	ok
evans	6867	none	login evans	ok
evans	6956	evans	emacs csclass	519
evans	6962	evans	logout	ok
farmer	3954	none	login farmer	fail
farmer	3966	none	login farmer	fail
farmer	3974	none	login farmer	fail
farmer	3985	none	login farmer	ok
farmer	3990	farmer	su	fail
farmer	3996	farmer	su	fail
farmer	4015	farmer	su	fail
farmer	4026	farmer	su	fail
farmer	4028	farmer	su	fail
farmer	4032	farmer	su	fail
farmer	4039	farmer	su	fail
farmer	4056	farmer	su	ok
farmer	4057	farmer	cd ~adams	ok
farmer	4064	adams	ls	ok
farmer	4083	adams	cd ~dog	ok
farmer	4105	dog	ls	ok
farmer	4123	dog	cd ~adams	ok
farmer	4137	adams	cd ~tom/ba	ok
farmer	4144	ba	cd ~farmer	ok
farmer	4152	farmer	ls	fail
farmer	4184	farmer	ls	ok
farmer	4195	farmer	cd ~graham	ok
farmer	4210	graham	ls	ok
farmer	4217	graham	cd ~root	ok
farmer	4232	root	ls	ok
farmer	4234	root	cd ~adams	ok

```
farmer     4252     adams            cat auxa      ok
farmer     4412     adams            cat auxb      ok
farmer     4494     adams            cat auxc      ok
farmer     4710     adams         cat diradams     ok
farmer     4719     adams           cd ~tom/ba     ok
farmer     4720     ba             cd ~root/bin     ok
farmer     4738     bin              cd ~graham     ok
farmer     4836     graham       cat important     ok
farmer     4849     graham          cd ~farmer     ok
farmer     5002     farmer         cat secrets     ok
farmer     5005     farmer              logout     ok
graham     4098     graham     emacs important     10444
graham     4099     graham              logout     ok
graham     8088     none          login graham     ok
graham     8098     graham             cd ~tom     ok
graham     8121     tom                    ls      ok
graham     8266     tom              mail root     bad(cd,bin)
graham     8855     tom               emacs aa     549
graham     8858     tom                 logout     ok
jones      1680     none           login jones     ok
jones      1681     jones            cd ~smith     ok
jones      1716     smith                  ls      ok
jones      1818     smith          login smith     ok
jones      5359     none           login jones     ok
jones      5377     jones              cd ~doe     ok
jones      5386     doe                    ls      ok
jones      5435     doe              mail root     bad(cd,bin)
jones      5798     doe         emacs bigpaper     29935
jones      5798     doe                 logout     ok
root       3755     root                cd etc     ok
root       3796     etccp passwd ~smith/dont_dare_look_at_this     ok
root       3974     etc              mail root     Captain Flash strikes again!!!!
root       3978     etc                 logout     ok
root       5006     none            login root     fail
root       5010     none            login root     fail
root       5014     none            login root     fail
root       5016     none            login root     fail
root       5021     none            login root     fail
root       5030     none            login root     ok
root       5045     root          cd ~root/bin     ok
root       5051     bin                    ls      fail
root       5071     bin                    ls      ok
root       5079     bin              cd ~adams     ok
root       5094     adams           cd ~tom/ba     ok
root       5096     ba       cd ~evans/csclass     ok
root       5108     csclass          cd ~davis     ok
root       5128     davis  cd ~adams/diradams     ok
root       5143     diradams           cd ~doe     ok
root       5147     doe                cd ~dog     ok
root       5186     dog                    ls      fail
root       5214     dog                    ls      fail
root       5246     dog                    ls      ok
root       5249     dog              cd ~adams     ok
root       5257     adams           cd ~tom/ba     ok
root       5275     ba                 cd ~tom     ok
root       5276     tom                    ls      ok
root       5284     tom              cd ~adams     ok
root       5294     adams           cd ~tom/ba     ok
root       5310     ba             cd ~root/bin     ok
root       5311     bin      cd ~evans/csclass     ok
root       5322     csclass            cd ~uri     ok
```

```
root        5335      uri                    ls      ok
root        5344      uri             cd ~adams      ok
root        5355      adams           cd ~tom/ba     ok
root        5371      ba            cd ~root/bin     ok
root        5374      bin                cd ~tom      ok
root        5394      tom                   rm *      ok
root        5417      tom              mail tom      Haha ful
root        5419      tom                logout      ok
smith       2368      smith       emacs tmp1434      344
smith       3000      smith       emacs tmp1435      362
smith       3465      smith       emacs tmp1436      405
smith       3473      smith              logout      ok
uri         3550      none            login uri      ok
uri         3561      uri             cd ~adams      ok
uri         3569      adams         cd ~root/bin     ok
uri         3602      bin                    ls      ok
uri         3609      bin             cd ~adams      ok
uri         3626      adams            cd ~root      ok
uri         3634      root                   ls      fail
uri         3646      root                   ls      fail
uri         3677      root                   ls      fail
uri         3680      root                   ls      ok
uri         3691      root           login root      fail
uri         3699      root           login root      fail
uri         3704      root           login root      fail
uri         3705      root           login root      fail
uri         3708      root           login root      fail
uri         3722      root           login root      fail
uri         3735      root           login root      ok

*******************************************************************************
*                                                                             *
*                                MAIL RECEIVED                                *
*                                                                             *
*      The following displays mail received by root:                          *
*                                                                             *
*******************************************************************************


From        To      Time        Problem(File,Directory)

adams       root    5709        bad(cd,bin)
brown       root    5455        bad(cd,bin)
dog         root    4906        bad(bb,tom)
graham      root    8266        bad(cd,bin)
jones       root    5435        bad(cd,bin)
root        root    3974        Captain Flash strikes again!!!!

% Undefined procedures will just fail ('fail' option)
Warnings:
This fact is not removable: changed(password,root)
This fact is not removable: confronted(user,_14653)
This fact is not removable: examined(password,_14587)
This fact is not removable: executed(password,cracker)
This fact is not removable: investigated(password,_14566)
This fact is not removable: changed(password,for,_14524)
This fact is not removable: changed(permissions,file,_14696)
This fact is not removable: restored(password,for,_14632)
This fact is not removable: issued(new,password,to,_14610)
```

```
Your objectives:
backup tape is stored and password cracker is executed.
Wait a moment while I analyze the problem thoroughly.

*************************************************************************
*                                                                       *
*  To see a list of possible actions, type the letter "h" or the word   *
*  "help." To review the audit file or your mail at anytime, type the   *
*  word "auditfile" or "mail" respectively.                             *
*                                                                       *
*************************************************************************
Type h for help.
************ These facts are now true: *************
backup tape is stored,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
and mail(root,root,3974,Captain Flash strikes again!!!!) is true.
Select an action: change root password
You chose to change root password.
OK, but a hint: "change permissions file passwd"
 is more important now than "change root password".
************ These facts are now true: *************
password root is changed,
backup tape is stored,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
and mail(root,root,3974,Captain Flash strikes again!!!!) is true.
Select an action: check permissions file passwd
You chose to check permissions file passwd.
OK.
************ These facts are now true: *************
password root is changed,
backup tape is stored,
checked(permissions,file,passwd) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
and mail(root,root,3974,Captain Flash strikes again!!!!) is true.
Select an action: change permissions file passwd
You chose to change permissions file passwd.
OK.
************ These facts are now true: *************
password root is changed,
backup tape is stored,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
and mail(root,root,3974,Captain Flash strikes again!!!!) is true.
Select an action: confront user dog
```

```
You chose to confront user dog.
OK, but a hint: "compare file cd for Trojan Horse with cd on backup tape"
 is more important now than "confront user dog".
************ These facts are now true: **************
password root is changed,
user dog is confronted,
backup tape is stored,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
and mail(root,root,3974,Captain Flash strikes again!!!!) is true.
Select an action: locate backup tape
You chose to locate backup tape.
OK.
************ These facts are now true: **************
password root is changed,
user dog is confronted,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
and mail(root,root,3974,Captain Flash strikes again!!!!) is true.
Select an action: load backup tape
You chose to load backup tape.
OK.
************ These facts are now true: **************
password root is changed,
user dog is confronted,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
and mail(root,root,3974,Captain Flash strikes again!!!!) is true.
Select an action: find file cd on backup tape
You chose to find file cd on backup tape.
OK.
************ These facts are now true: **************
password root is changed,
user dog is confronted,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
```

```
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
and found(file,cd,on,backup,tape) is true.
Select an action: compare file cd for Trojan Horse with cd on backup tape
You chose to compare file cd for Trojan Horse with cd on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user dog is confronted,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,cd,on,backup,tape) is true,
and compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true.
Select an action: execute password cracker
You chose to execute password cracker.
OK, but a hint: "compare file ls for Trojan Horse with ls on backup tape"
 is more important now than "execute password cracker".
************ These facts are now true: *************
password root is changed,
user dog is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,_356277) is true,
known(insecure,password,for,_356284) is true,
known(insecure,password,for,_356291) is true,
known(insecure,password,for,_356298) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,cd,on,backup,tape) is true,
and compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true.
Select an action: find file ls on backup tape
You chose to find file ls on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user dog is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
```

```
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
and compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true.
Select an action: compare file ls for Trojan Horse with ls on backup tape
You chose to compare file ls for Trojan Horse with ls on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user dog is confronted,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: examine user password dog
You chose to examine user password dog.
Have you confused that with the investigate user password dog action?
Your action is not what I would choose, but let us try it.
************ These facts are now true: *************
password root is changed,
user dog is confronted,
password dog is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: investigate user password dog
You chose to investigate user password dog.
```

```
OK.
************ These facts are now true: *************
password root is changed,
user dog is confronted,
password dog is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,dog) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: change password for adams
You chose to change password for adams.
OK, but a hint: "restore modified file bb from backup"
 is more important now than "change password for adams".
************ These facts are now true: *************
password root is changed,
user dog is confronted,
password dog is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(password,for,adams) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,dog) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: find file bb on backup tape
You chose to find file bb on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user dog is confronted,
password dog is examined,
```

```
password cracker is executed,
backup tape is loaded,
backup tape is located,
changed(password,for,adams) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,dog) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore modified file bb from backup
You chose to restore modified file bb from backup.
OK.
************ These facts are now true: *************
password root is changed,
user dog is confronted,
password dog is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file bb is restored,
changed(password,for,adams) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,dog) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore modified file cd from backup
You chose to restore modified file cd from backup.
OK.
************ These facts are now true: *************
password root is changed,
user dog is confronted,
password dog is examined,
password cracker is executed,
backup tape is loaded,
```

```
backup tape is located,
file bb is restored,
file cd is restored,
changed(password,for,adams) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,dog) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: change user password smith
You chose to change user password smith.
Not a valid action.
********** These facts are now true: **********
password root is changed,
user dog is confronted,
password dog is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file bb is restored,
file cd is restored,
changed(password,for,adams) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,dog) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: change password for smith
You chose to change password for smith.
OK, but a hint: "restore deleted file aa from backup"
 is more important now than "change password for smith".
********** These facts are now true: **********
password root is changed,
user dog is confronted,
password dog is examined,
```

```
password cracker is executed,
backup tape is loaded,
backup tape is located,
file bb is restored,
file cd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,dog) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: find file aa on backup tape
You chose to find file aa on backup tape.
OK.
************ These facts are now true: **************
password root is changed,
user dog is confronted,
password dog is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file bb is restored,
file cd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,dog) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore deleted file aa from backup
You chose to restore deleted file aa from backup.
OK.
```

```
************ These facts are now true: *************
password root is changed,
user dog is confronted,
password dog is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file aa is restored,
file bb is restored,
file cd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,dog) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore deleted file bb from backup
You chose to restore deleted file bb from backup.
OK.
************ These facts are now true: *************
password root is changed,
user dog is confronted,
password dog is examined,
password cracker is executed,
backup tape is loaded,
backup tape is located,
file aa is restored,
file bb is restored,
file cd is restored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,dog) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
```

```
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: store backup tape
You chose to store backup tape.
OK, but a hint: "change password for farmer"
 is more important now than "store backup tape".
************ These facts are now true: *************
password root is changed,
user dog is confronted,
password dog is examined,
password cracker is executed,
file aa is restored,
file bb is restored,
file cd is restored,
backup tape is stored,
changed(password,for,adams) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,dog) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: change password for farmer
You chose to change password for farmer.
OK.
************ These facts are now true: *************
password root is changed,
user dog is confronted,
password dog is examined,
password cracker is executed,
file aa is restored,
file bb is restored,
file cd is restored,
backup tape is stored,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(password,for,smith) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
investigated(user,password,dog) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(adams,root,5709,bad(cd,bin)) is true,
```

```
mail(brown,root,5455,bad(cd,bin)) is true,
mail(dog,root,4906,bad(bb,tom)) is true,
mail(graham,root,8266,bad(cd,bin)) is true,
mail(jones,root,5435,bad(cd,bin)) is true,
mail(root,root,3974,Captain Flash strikes again!!!!) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: change password for graham
You chose to change password for graham.
OK.
Congratulations! You have done the job.
The session is over.  Do "go." to restart.

yes
| ?- statistics.

memory (total)          2484704 bytes:    1331300 in use,    1153404 free
   program space        1200236 bytes
   global space           65532 bytes:      27348 in use,      38184 free
      global stack                          25220 bytes
      trail                                    40 bytes
      system                                 2088 bytes
   local stack            65532 bytes:        648 in use,      64884 free
      local stack                           624 bytes
      system                                 24 bytes

 16.017 sec. for 0 global and 30 local space shifts
 0.234 sec. for 1 garbage collections which collected 992596 bytes
 47.066 sec. runtime

yes
| ?- halt.
```

TAB 4. RUN 3

The following is the audit file used for Run 4:

```
audit(jones,338,none,'login jones',fail).
audit(jones,347,none,'login jones',fail).
audit(jones,355,none,'login jones',fail).
audit(jones,361,none,'login jones',fail).
audit(jones,363,none,'login jones',fail).
audit(jones,372,none,'login jones',fail).
audit(jones,385,none,'login jones',fail).
audit(jones,387,none,'login jones',fail).
audit(jones,394,none,'login jones',fail).
audit(jones,402,none,'login jones',fail).
audit(jones,413,none,'login jones',fail).
audit(jones,426,none,'login jones',ok).
audit(jones,433,jones,'cd ~root/bin',ok).
audit(jones,451,bin,ls,ok).
audit(jones,462,bin,'cd ~root',ok).
audit(jones,475,root,ls,ok).
audit(jones,481,root,'login root',fail).
audit(jones,489,root,'login root',fail).
audit(jones,495,root,'login root',fail).
audit(jones,501,root,'login root',fail).
audit(jones,514,root,'login root',ok).
audit(root,518,root,'cd ~adams',ok).
audit(root,533,adams,'cd ~tom/ba',ok).
audit(root,537,ba,'cd bin',ok).
audit(root,537,bin,'cd ~evans/csclass',ok).
audit(root,549,csclass,'cd ~root/etc',ok).
audit(root,557,etc,'cp passwd ~smith/dont_dare_look_at_this',ok).
audit(root,569,etc,'mail root','Captain Flash strikes again!!!!').
audit(root,576,etc,logout,ok).
audit(brown,1691,none,'login brown',ok).
audit(evans,1693,none,'login evans',ok).
audit(brown,1708,brown,'cd ~adams',ok).
audit(brown,1711,adams,'cd ~tom/ba',ok).
audit(brown,1726,ba,'cd ~root/bin',ok).
audit(brown,1730,bin,'cd ~evans/csclass',ok).
audit(brown,1734,csclass,'cd ~davis',ok).
audit(brown,1741,davis,'cd ~adams/diradams',ok).
audit(brown,1744,diradams,'cd ~doe',ok).
audit(brown,1752,doe,'cd ~tom',ok).
audit(tom,1843,none,'login tom',ok).
audit(tom,1845,tom,'cd ~adams',ok).
audit(tom,1859,adams,'cd ba',ok).
audit(tom,1872,ba,'cd ~root/bin',ok).
audit(tom,1905,bin,ls,ok).
audit(tom,2091,bin,'cd ~adams',ok).
audit(tom,2106,adams,'cd ba',ok).
audit(evans,2109,evans,'cd csclass',ok).
audit(evans,2109,csclass,logout,ok).
audit(tom,2126,ba,'cd ~graham',ok).
audit(tom,2160,graham,ls,ok).
audit(graham,2171,none,'login graham',fail).
audit(graham,2172,none,'login graham',fail).
audit(graham,2176,none,'login graham',ok).
audit(graham,2177,graham,'cd ~root/bin',ok).
```

```
audit(tom,2184,graham,'login graham',ok).
audit(graham,2194,bin,ls,fail).
audit(brown,2212,tom,'emacs bb',587).
audit(graham,2213,bin,ls,ok).
audit(graham,2214,bin,'cd ~dog',ok).
audit(graham,2249,dog,ls,fail).
audit(graham,2253,graham,'emacs important',10360).
audit(graham,2255,dog,ls,fail).
audit(graham,2260,graham,logout,ok).
audit(graham,2273,dog,ls,ok).
audit(graham,2292,dog,'cd ~adams',ok).
audit(graham,2302,adams,'cd ~tom/ba',ok).
audit(graham,2311,ba,'cd ~root/bin',ok).
audit(graham,2321,bin,'cd ~tom',ok).
audit(farmer,2330,none,'login farmer',ok).
audit(graham,2330,tom,ls,ok).
audit(farmer,2340,farmer,'cd ~adams',ok).
audit(graham,2342,tom,'cd ~adams',ok).
audit(farmer,2352,adams,'cd ~smith',ok).
audit(graham,2360,adams,'cd ~tom/ba',ok).
audit(davis,2363,none,'login davis',ok).
audit(graham,2367,ba,'cd ~uri',ok).
audit(graham,2376,uri,ls,ok).
audit(brown,2382,tom,'mail root',bad(bb,tom)).
audit(graham,2382,uri,'cd ~adams',ok).
audit(brown,2383,tom,logout,ok).
audit(farmer,2384,smith,ls,ok).
audit(graham,2391,adams,'cd ~tom',ok).
audit(farmer,2414,smith,'login smith',fail).
audit(farmer,2422,smith,'login smith',ok).
audit(graham,2429,tom,'rm *',ok).
audit(graham,2439,tom,'mail tom','Haha ful').
audit(graham,2444,tom,logout,ok).
audit(smith,2651,smith,'emacs tmp1434',344).
audit(davis,2940,davis,'emacs goodnews',1526).
audit(davis,2945,davis,logout,ok).
audit(evans,3046,none,'login evans',ok).
audit(evans,3066,evans,'cd ~adams',ok).
audit(evans,3075,adams,'cd ~tom/ba',ok).
audit(evans,3094,ba,'cd ~root/bin',ok).
audit(evans,3106,bin,'cd ~evans/csclass',ok).
audit(evans,3115,csclass,'cd ~doe',ok).
audit(evans,3118,none,'login evans',ok).
audit(smith,3122,smith,'emacs tmp1435',362).
audit(evans,3128,evans,'cd ~tom',ok).
audit(evans,3136,doe,ls,ok).
audit(evans,3161,tom,ls,ok).
audit(evans,3205,tom,ls,ok).
audit(smith,3237,smith,'emacs tmp1436',405).
audit(smith,3239,smith,logout,ok).
audit(evans,3290,doe,ls,fail).
audit(evans,3328,doe,ls,ok).
audit(evans,3351,tom,'emacs aa',503).
audit(evans,3357,tom,logout,ok).
audit(evans,3475,doe,'emacs bigpaper',30095).
audit(evans,3477,doe,logout,ok).
audit(davis,5712,none,'login davis',ok).
audit(davis,6132,davis,'emacs topsecret',1572).
audit(davis,6134,davis,logout,ok).
audit(davis,7336,none,'login davis',fail).
audit(davis,7346,none,'login davis',fail).
```

```
audit(davis,7354,none,'login davis',fail).
audit(davis,7363,none,'login davis',fail).
audit(davis,7364,none,'login davis',fail).
audit(davis,7371,none,'login davis',fail).
audit(davis,7378,none,'login davis',fail).
audit(davis,7387,none,'login davis',fail).
audit(davis,7399,none,'login davis',fail).
audit(davis,7402,none,'login davis',fail).
audit(davis,7409,none,'login davis',fail).
audit(davis,7417,none,'login davis',ok).
audit(davis,7436,davis,su,fail).
audit(davis,7445,davis,su,fail).
audit(davis,7446,davis,su,fail).
audit(davis,7459,davis,su,fail).
audit(davis,7472,davis,su,fail).
audit(davis,7488,davis,su,fail).
audit(davis,7501,davis,su,fail).
audit(davis,7516,davis,su,fail).
audit(davis,7521,davis,su,fail).
audit(davis,7521,davis,su,ok).
audit(davis,7535,davis,'cd ~adams',ok).
audit(davis,7554,adams,ls,ok).
audit(davis,7574,adams,'cd ~dog',ok).
audit(davis,7606,dog,ls,fail).
audit(davis,7620,dog,ls,fail).
audit(davis,7624,dog,ls,fail).
audit(davis,7638,dog,ls,ok).
audit(davis,7656,dog,'cd ~farmer',ok).
audit(farmer,7665,none,'login farmer',ok).
audit(farmer,7678,farmer,'cd ~adams',ok).
audit(davis,7679,farmer,ls,ok).
audit(davis,7685,farmer,'cd ~adams',ok).
audit(davis,7695,adams,'cd ~tom/ba',ok).
audit(davis,7696,ba,'cd ~root/bin',ok).
audit(davis,7703,bin,'cd ~evans/csclass',ok).
audit(davis,7706,csclass,'cd ~davis',ok).
audit(davis,7715,davis,'cd ~adams/diradams',ok).
audit(farmer,7716,adams,ls,ok).
audit(davis,7732,diradams,'cd ~graham',ok).
audit(davis,7763,graham,ls,ok).
audit(davis,7779,graham,'cd ~adams',ok).
audit(davis,7797,adams,'cd ~tom/ba',ok).
audit(davis,7799,ba,'cd ~root/bin',ok).
audit(davis,7808,bin,'cd ~evans/csclass',ok).
audit(davis,7820,csclass,'cd ~root',ok).
audit(davis,7823,root,ls,ok).
audit(davis,7827,root,'cd ~adams',ok).
audit(farmer,7877,adams,ls,ok).
audit(farmer,7883,adams,'login adams',ok).
audit(adams,7886,adams,'cd ~adams',ok).
audit(adams,7896,adams,'cd ~tom/ba',ok).
audit(adams,7911,ba,'cd ~adams/diradams',ok).
audit(davis,7936,adams,'cat auxa',ok).
audit(davis,8071,adams,'cat auxb',ok).
audit(davis,8182,adams,'cat auxc',ok).
audit(davis,8217,adams,'cat diradams',ok).
audit(davis,8229,adams,'cd ~graham',ok).
audit(davis,8247,graham,'cat important',ok).
audit(davis,8254,graham,'cd ~farmer',ok).
audit(adams,8260,diradams,'emacs auxb',1134).
audit(davis,8445,farmer,'cat secrets',ok).
```

```
audit(davis,8447,farmer,logout,ok).
audit(adams,8519,diradams,'emacs auxc',5118).
audit(adams,8520,diradams,logout,ok).
audit(jones,9008,none,'login jones',fail).
audit(jones,9015,none,'login jones',fail).
audit(jones,9019,none,'login jones',fail).
audit(jones,9032,none,'login jones',fail).
audit(jones,9043,none,'login jones',ok).
audit(jones,9049,jones,su,fail).
audit(jones,9058,jones,su,fail).
audit(jones,9069,jones,su,fail).
audit(jones,9085,jones,su,fail).
audit(jones,9090,jones,su,fail).
audit(jones,9107,jones,su,fail).
audit(jones,9115,jones,su,fail).
audit(jones,9123,jones,su,fail).
audit(jones,9133,jones,su,fail).
audit(jones,9149,jones,su,ok).
audit(jones,9163,jones,'cd ~adams',ok).
audit(jones,9165,adams,'cd ~root/bin',ok).
audit(jones,9190,bin,ls,ok).
audit(jones,9200,bin,'cd ~adams',ok).
audit(jones,9203,adams,'cd ~root',ok).
audit(jones,9218,root,ls,ok).
audit(jones,9228,root,'cd ~adams',ok).
audit(jones,9240,adams,'cd ~root/bin',ok).
audit(jones,9441,bin,'emacs cd',5109).
audit(jones,9560,bin,'emacs ls',2133).
audit(jones,9776,bin,'emacs please_run_me',22914).
audit(jones,9781,bin,logout,ok).
audit(jones,9789,bin,'login jones',ok).
audit(jones,9808,jones,'cd ~root/bin',ok).
audit(jones,10393,bin,'emacs please_run_me',22914).
audit(jones,10401,bin,logout,ok).
```

The following is the script of Run 4:

```
Script started on Wed Mar 15 22:56:06 1995
.alias: No such file or directory.
[7mai2:/users/work4/schiavo/Thesis/Tutor>>[mprolog


Quintus Prolog Release 3.1.1 (Sun-4, SunOS 4.0)
Copyright (C) 1990, Quintus Corporation.  All rights reserved.
2100 Geng Road, Palo Alto, California U.S.A. (415) 813-3800

| ?- [intruder].
% compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/intruder.pl
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/metutor30.pl
% Undefined procedures will just fail ('fail' option)
%    loading file /usr/local/q3.1.1/generic/qplib3.1.1/library/random.qof
%     foreign file /usr/local/q3.1.1/generic/qplib3.1.1/library/sun4-4/libpl.so loaded
%    random.qof loaded, 0.133 sec 9,392 bytes
%    module random imported into user
* Clauses for writefact/2 are not together in the source file
%  metutor30.pl compiled in module user, 3.000 sec 50,420 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/modrowe7
%  modrowe7 compiled in module user, 0.684 sec 15,720 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/filetree
```

```
%  filetree compiled in module user, 0.434 sec 5,296 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/rules
* Clauses for behavior/5 are not together in the source file
* Clauses for behavior/4 are not together in the source file
%  rules compiled in module user, 0.617 sec 7,456 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/rowefiles
%  rowefiles compiled in module user, 0.117 sec 4,256 bytes
%  compiling file /tmp_mnt/users/work4/schiavo/Thesis/Tutor/operators
* Clauses for recommended/3 are not together in the source file
* Clauses for recommended/2 are not together in the source file
* Clauses for addpostcondition/2 are not together in the source file
%  operators compiled in module user, 0.600 sec 8,348 bytes
% intruder.pl compiled in module user, 6.350 sec 102,384 bytes

yes
| ?- statistics.

memory (total)          649696 bytes:     466020 in use,     183676 free
   program space        334956 bytes
   global space          65532 bytes:      26688 in use,      38844 free
      global stack                         24584 bytes
      trail                                   16 bytes
      system                                2088 bytes
   local stack           65532 bytes:        440 in use,      65092 free
      local stack                           416 bytes
      system                                 24 bytes

 0.000 sec. for 0 global and 3 local space shifts
 0.000 sec. for 0 garbage collections which collected 0 bytes
 6.633 sec. runtime

yes
| ?- start.

*********************************************************************************
*                                                                               *
*                                  AUDIT FILE                                   *
*                                                                               *
*      The following displays the current contents of the audit file:           *
*                                                                               *
*********************************************************************************


Name        Time      Path             Command        Result

adams       7886      adams             cd ~adams      ok
adams       7896      adams            cd ~tom/ba      ok
adams       7911      ba      cd ~adams/diradams      ok
adams       8260      diradams        emacs auxb      1134
adams       8519      diradams        emacs auxc      5118
adams       8520      diradams            logout      ok
brown       1691      none           login brown      ok
brown       1708      brown             cd ~adams      ok
brown       1711      adams            cd ~tom/ba      ok
brown       1726      ba             cd ~root/bin      ok
brown       1730      bin      cd ~evans/csclass      ok
brown       1734      csclass          cd ~davis      ok
brown       1741      davis  cd ~adams/diradams      ok
brown       1744      diradams           cd ~doe      ok
brown       1752      doe                cd ~tom      ok
brown       2212      tom               emacs bb      587
```

brown	2382	tom	mail root	bad(bb,tom)
brown	2383	tom	logout	ok
davis	2363	none	login davis	ok
davis	2940	davis	emacs goodnews	1526
davis	2945	davis	logout	ok
davis	5712	none	login davis	ok
davis	6132	davis	emacs topsecret	1572
davis	6134	davis	logout	ok
davis	7336	none	login davis	fail
davis	7346	none	login davis	fail
davis	7354	none	login davis	fail
davis	7363	none	login davis	fail
davis	7364	none	login davis	fail
davis	7371	none	login davis	fail
davis	7378	none	login davis	fail
davis	7387	none	login davis	fail
davis	7399	none	login davis	fail
davis	7402	none	login davis	fail
davis	7409	none	login davis	fail
davis	7417	none	login davis	ok
davis	7436	davis	su	fail
davis	7445	davis	su	fail
davis	7446	davis	su	fail
davis	7459	davis	su	fail
davis	7472	davis	su	fail
davis	7488	davis	su	fail
davis	7501	davis	su	fail
davis	7516	davis	su	fail
davis	7521	davis	su	fail
davis	7521	davis	su	ok
davis	7535	davis	cd ~adams	ok
davis	7554	adams	ls	ok
davis	7574	adams	cd ~dog	ok
davis	7606	dog	ls	fail
davis	7620	dog	ls	fail
davis	7624	dog	ls	fail
davis	7638	dog	ls	ok
davis	7656	dog	cd ~farmer	ok
davis	7679	farmer	ls	ok
davis	7685	farmer	cd ~adams	ok
davis	7695	adams	cd ~tom/ba	ok
davis	7696	ba	cd ~root/bin	ok
davis	7703	bin	cd ~evans/csclass	ok
davis	7706	csclass	cd ~davis	ok
davis	7715	davis	cd ~adams/diradams	ok
davis	7732	diradams	cd ~graham	ok
davis	7763	graham	ls	ok
davis	7779	graham	cd ~adams	ok
davis	7797	adams	cd ~tom/ba	ok
davis	7799	ba	cd ~root/bin	ok
davis	7808	bin	cd ~evans/csclass	ok
davis	7820	csclass	cd ~root	ok
davis	7823	root	ls	ok
davis	7827	root	cd ~adams	ok
davis	7936	adams	cat auxa	ok
davis	8071	adams	cat auxb	ok
davis	8182	adams	cat auxc	ok
davis	8217	adams	cat diradams	ok
davis	8229	adams	cd ~graham	ok
davis	8247	graham	cat important	ok
davis	8254	graham	cd ~farmer	ok

davis	8445	farmer	cat secrets	ok
davis	8447	farmer	logout	ok
evans	1693	none	login evans	ok
evans	2109	csclass	logout	ok
evans	2109	evans	cd csclass	ok
evans	3046	none	login evans	ok
evans	3066	evans	cd ~adams	ok
evans	3075	adams	cd ~tom/ba	ok
evans	3094	ba	cd ~root/bin	ok
evans	3106	bin	cd ~evans/csclass	ok
evans	3115	csclass	cd ~doe	ok
evans	3118	none	login evans	ok
evans	3128	evans	cd ~tom	ok
evans	3136	doe	ls	ok
evans	3161	tom	ls	ok
evans	3205	tom	ls	ok
evans	3290	doe	ls	fail
evans	3328	doe	ls	ok
evans	3351	tom	emacs aa	503
evans	3357	tom	logout	ok
evans	3475	doe	emacs bigpaper	30095
evans	3477	doe	logout	ok
farmer	2330	none	login farmer	ok
farmer	2340	farmer	cd ~adams	ok
farmer	2352	adams	cd ~smith	ok
farmer	2384	smith	ls	ok
farmer	2414	smith	login smith	fail
farmer	2422	smith	login smith	ok
farmer	7665	none	login farmer	ok
farmer	7678	farmer	cd ~adams	ok
farmer	7716	adams	ls	ok
farmer	7877	adams	ls	ok
farmer	7883	adams	login adams	ok
graham	2171	none	login graham	fail
graham	2172	none	login graham	fail
graham	2176	none	login graham	ok
graham	2177	graham	cd ~root/bin	ok
graham	2194	bin	ls	fail
graham	2213	bin	ls	ok
graham	2214	bin	cd ~dog	ok
graham	2249	dog	ls	fail
graham	2253	graham	emacs important	10360
graham	2255	dog	ls	fail
graham	2260	graham	logout	ok
graham	2273	dog	ls	ok
graham	2292	dog	cd ~adams	ok
graham	2302	adams	cd ~tom/ba	ok
graham	2311	ba	cd ~root/bin	ok
graham	2321	bin	cd ~tom	ok
graham	2330	tom	ls	ok
graham	2342	tom	cd ~adams	ok
graham	2360	adams	cd ~tom/ba	ok
graham	2367	ba	cd ~uri	ok
graham	2376	uri	ls	ok
graham	2382	uri	cd ~adams	ok
graham	2391	adams	cd ~tom	ok
graham	2429	tom	rm *	ok
graham	2439	tom	mail tom	Haha ful
graham	2444	tom	logout	ok
jones	338	none	login jones	fail
jones	347	none	login jones	fail

```
jones      355    none          login jones     fail
jones      361    none          login jones     fail
jones      363    none          login jones     fail
jones      372    none          login jones     fail
jones      385    none          login jones     fail
jones      387    none          login jones     fail
jones      394    none          login jones     fail
jones      402    none          login jones     fail
jones      413    none          login jones     fail
jones      426    none          login jones     ok
jones      433    jones       cd ~root/bin      ok
jones      451    bin                 ls        ok
jones      462    bin           cd ~root        ok
jones      475    root                ls        ok
jones      481    root          login root      fail
jones      489    root          login root      fail
jones      495    root          login root      fail
jones      501    root          login root      fail
jones      514    root          login root      ok
jones     9008    none          login jones     fail
jones     9015    none          login jones     fail
jones     9019    none          login jones     fail
jones     9032    none          login jones     fail
jones     9043    none          login jones     ok
jones     9049    jones               su        fail
jones     9058    jones               su        fail
jones     9069    jones               su        fail
jones     9085    jones               su        fail
jones     9090    jones               su        fail
jones     9107    jones               su        fail
jones     9115    jones               su        fail
jones     9123    jones               su        fail
jones     9133    jones               su        fail
jones     9149    jones               su        ok
jones     9163    jones         cd ~adams       ok
jones     9165    adams       cd ~root/bin      ok
jones     9190    bin                 ls        ok
jones     9200    bin           cd ~adams       ok
jones     9203    adams          cd ~root       ok
jones     9218    root                ls        ok
jones     9228    root          cd ~adams       ok
jones     9240    adams       cd ~root/bin      ok
jones     9441    bin              emacs cd     5109
jones     9560    bin              emacs ls     2133
jones     9776    bin   emacs please_run_me     22914
jones     9781    bin               logout      ok
jones     9789    bin         login jones       ok
jones     9808    jones       cd ~root/bin      ok
jones    10393    bin   emacs please_run_me     22914
jones    10401    bin               logout      ok
root       518    root          cd ~adams       ok
root       533    adams         cd ~tom/ba      ok
root       537    ba                cd bin      ok
root       537    bin     cd ~evans/csclass     ok
root       549    csclass     cd ~root/etc      ok
root       557    etccp passwd ~smith/dont_dare_look_at_this     ok
root       569    etc             mail root     Captain Flash strikes again!!!!
root       576    etc               logout      ok
smith     2651    smith       emacs tmp1434     344
smith     3122    smith       emacs tmp1435     362
smith     3237    smith       emacs tmp1436     405
```

```
smith       3239      smith              logout      ok
tom         1843      none             login tom     ok
tom         1845      tom              cd ~adams     ok
tom         1859      adams                cd ba     ok
tom         1872      ba           cd ~root/bin      ok
tom         1905      bin                    ls      ok
tom         2091      bin              cd ~adams     ok
tom         2106      adams                cd ba     ok
tom         2126      ba             cd ~graham      ok
tom         2160      graham                 ls      ok
tom         2184      graham       login graham      ok


*******************************************************************************
*                                                                             *
*                                  MAIL RECEIVED                              *
*                                                                             *
*      The following displays mail received by root:                          *
*                                                                             *
*******************************************************************************


From         To       Time        Problem(File,Directory)

brown       root      2382        bad(bb,tom)
root        root      569         Captain Flash strikes again!!!!

% Undefined procedures will just fail ('fail' option)
Warnings:
This fact is not removable: changed(password,root)
This fact is not removable: confronted(user,_12821)
This fact is not removable: examined(password,_12755)
This fact is not removable: executed(password,cracker)
This fact is not removable: investigated(password,_12734)
This fact is not removable: changed(password,for,_12692)
This fact is not removable: changed(permissions,file,_12864)
This fact is not removable: restored(password,for,_12800)
This fact is not removable: issued(new,password,to,_12778)

Your objectives:
backup tape is stored and password cracker is executed.
Wait a moment while I analyze the problem thoroughly.

*************************************************************************
*                                                                       *
*  To see a list of possible actions, type the letter "h" or the word   *
*  "help." To review the audit file or your mail at anytime, type the   *
*  word "auditfile" or "mail" respectively.                             *
*                                                                       *
*************************************************************************
Type h for help.
************ These facts are now true: *************
backup tape is stored,
mail(brown,root,2382,bad(bb,tom)) is true,
and mail(root,root,569,Captain Flash strikes again!!!!) is true.
Select an action: check permissions file passwd
You chose to check permissions file passwd.
OK.
************ These facts are now true: *************
backup tape is stored,
checked(permissions,file,passwd) is true,
```

```
mail(brown,root,2382,bad(bb,tom)) is true,
and mail(root,root,569,Captain Flash strikes again!!!!) is true.
Select an action: change permissions passwd
You chose to change permissions passwd.
Not a valid action.
************ These facts are now true: *************
backup tape is stored,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
and mail(root,root,569,Captain Flash strikes again!!!!) is true.
Select an action: change permissions file passwd
You chose to change permissions file passwd.
OK.
************ These facts are now true: *************
backup tape is stored,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
and mail(root,root,569,Captain Flash strikes again!!!!) is true.
Select an action: change root password
You chose to change root password.
OK.
************ These facts are now true: *************
password root is changed,
backup tape is stored,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
and mail(root,root,569,Captain Flash strikes again!!!!) is true.
Select an action: confront user davis
You chose to confront user davis.
OK, but a hint: "compare file cd for Trojan Horse with cd on backup tape"
 is more important now than "confront user davis".
************ These facts are now true: *************
password root is changed,
user davis is confronted,
backup tape is stored,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
and mail(root,root,569,Captain Flash strikes again!!!!) is true.
Select an action: locate backup tape
You chose to locate backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user davis is confronted,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
and mail(root,root,569,Captain Flash strikes again!!!!) is true.
Select an action: load backup tape
You chose to load backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user davis is confronted,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
```

```
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
and mail(root,root,569,Captain Flash strikes again!!!!) is true.
Select an action: find file cd on backup tape
You chose to find file cd on backup tape.
OK.
************ These facts are now true: **************
password root is changed,
user davis is confronted,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
mail(root,root,569,Captain Flash strikes again!!!!) is true,
and found(file,cd,on,backup,tape) is true.
Select an action: compare file cd for Trojan Horse with cd on backup tape
You chose to compare file cd for Trojan Horse with cd on backup tape.
OK.
************ These facts are now true: **************
password root is changed,
user davis is confronted,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
mail(root,root,569,Captain Flash strikes again!!!!) is true,
found(file,cd,on,backup,tape) is true,
and compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true.
Select an action: find file ls on backup tape
You chose to find file ls on backup tape.
OK.
************ These facts are now true: **************
password root is changed,
user davis is confronted,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
mail(root,root,569,Captain Flash strikes again!!!!) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
and compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true.
Select an action: compare file ls for Trojan Horse with ls on backup tape
You chose to compare file ls for Trojan Horse with ls on backup tape.
OK.
************ These facts are now true: **************
password root is changed,
user davis is confronted,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
mail(root,root,569,Captain Flash strikes again!!!!) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
```

```
Select an action: find file bb on backup tape
You chose to find file bb on backup tape.
Have you confused that with the find file aa on backup tape action?
OK, but a hint: "restore deleted file aa from backup"
 is more important now than "restore deleted file bb from backup".
************ These facts are now true: *************
password root is changed,
user davis is confronted,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
mail(root,root,569,Captain Flash strikes again!!!!) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: find file aa on backup tape
You chose to find file aa on backup tape.
OK.
************ These facts are now true: *************
password root is changed,
user davis is confronted,
backup tape is loaded,
backup tape is located,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
mail(root,root,569,Captain Flash strikes again!!!!) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore deleted file aa from backup
You chose to restore deleted file aa from backup.
OK.
************ These facts are now true: *************
password root is changed,
user davis is confronted,
backup tape is loaded,
backup tape is located,
file aa is restored,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
mail(root,root,569,Captain Flash strikes again!!!!) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: restore deleted file bb from backup
You chose to restore deleted file bb from backup.
OK.
************ These facts are now true: *************
password root is changed,
```

```
user davis is confronted,
backup tape is loaded,
backup tape is located,
file aa is restored,
file bb is restored,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
mail(root,root,569,Captain Flash strikes again!!!!) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: store backup tape
You chose to store backup tape.
OK, but a hint: "execute password cracker"
 is more important now than "store backup tape".
************ These facts are now true: *************
password root is changed,
user davis is confronted,
file aa is restored,
file bb is restored,
backup tape is stored,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
mail(root,root,569,Captain Flash strikes again!!!!) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: execute password cracker
You chose to execute password cracker.
OK.
************ These facts are now true: *************
password root is changed,
user davis is confronted,
password cracker is executed,
file aa is restored,
file bb is restored,
backup tape is stored,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,_434196) is true,
known(insecure,password,for,_434203) is true,
known(insecure,password,for,_434210) is true,
known(insecure,password,for,_434217) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
mail(root,root,569,Captain Flash strikes again!!!!) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: change password for adams
You chose to change password for adams.
```

```
OK.
************ These facts are now true: *************
password root is changed,
user davis is confronted,
password cracker is executed,
file aa is restored,
file bb is restored,
backup tape is stored,
changed(password,for,adams) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
mail(root,root,569,Captain Flash strikes again!!!!) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: change password for farmer
You chose to change password for farmer.
OK.
************ These facts are now true: *************
password root is changed,
user davis is confronted,
password cracker is executed,
file aa is restored,
file bb is restored,
backup tape is stored,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
mail(root,root,569,Captain Flash strikes again!!!!) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: change password for graham
You chose to change password for graham.
OK.
************ These facts are now true: *************
password root is changed,
user davis is confronted,
password cracker is executed,
file aa is restored,
file bb is restored,
backup tape is stored,
changed(password,for,adams) is true,
changed(password,for,farmer) is true,
```

```
changed(password,for,graham) is true,
changed(permissions,file,passwd) is true,
checked(permissions,file,passwd) is true,
known(insecure,password,for,adams) is true,
known(insecure,password,for,farmer) is true,
known(insecure,password,for,graham) is true,
known(insecure,password,for,smith) is true,
mail(brown,root,2382,bad(bb,tom)) is true,
mail(root,root,569,Captain Flash strikes again!!!!) is true,
found(file,aa,on,backup,tape) is true,
found(file,bb,on,backup,tape) is true,
found(file,cd,on,backup,tape) is true,
found(file,ls,on,backup,tape) is true,
compared(file,cd,for,Trojan Horse,with,cd,on,backup,tape) is true,
and compared(file,ls,for,Trojan Horse,with,ls,on,backup,tape) is true.
Select an action: change password for smith
You chose to change password for smith.
OK.
Congratulations! You have done the job.
The session is over.  Do "go." to restart.

yes
| ?- statistics.

memory (total)          2222560 bytes:    1043272 in use,    1179288 free
   program space         912208 bytes
   global space           65532 bytes:      28472 in use,      37060 free
      global stack                          26344 bytes
      trail                                    40 bytes
      system                                 2088 bytes
   local stack            65532 bytes:        648 in use,      64884 free
      local stack                           624 bytes
      system                                 24 bytes

 17.000 sec. for 0 global and 26 local space shifts
 0.000 sec. for 0 garbage collections which collected 0 bytes
 33.583 sec. runtime

yes
| ?- halt.
```

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center — 2
   Cameron Station
   Alexandria, VA 22304-6145

2. Dudley Knox Library — 2
   Code 52
   Naval Postgraduate School
   Monterey, CA 93943-5101

3. Chairman, Code CS — 2
   Computer Science Department
   Naval Postgraduate School
   Monterey, CA 93943

4. Prof. Neil C. Rowe, Code CS/Rp — 2
   Computer Science Department
   Naval Postgraduate School
   Monterey, CA 93943

5. Prof. Timothy J. Shimeall, Code CS/SM — 2
   Computer Science Department
   Naval Postgraduate School
   Monterey, CA 93943

6. Lt Sandra J. Schiavo — 2
   PSC 825 Box 58
   FPO AE 09627