3

Security

Security is quickly becoming one of the administrator's primary concerns as networks continue to grow in both numbers and diversity. ENlighten/DSM helps you integrate security capabilities, ensuring system and network integrity. The Security menu contains the following security auditing checks:

- Vital Files
- Filesystem Devices
- Boot and Shutdown Script Checks
- Crontab Contents
- Password File Integrity
- Group File Integrity
- User Home Directories
- Attempted Break-ins
- Obvious Passwords

Each of these security checks, except for Obvious Passwords, appends its findings to a security logfile, shown in Figure 3-1. You can use the Clear Log button to flush the logfile and the Print button to print the logfile as needed.

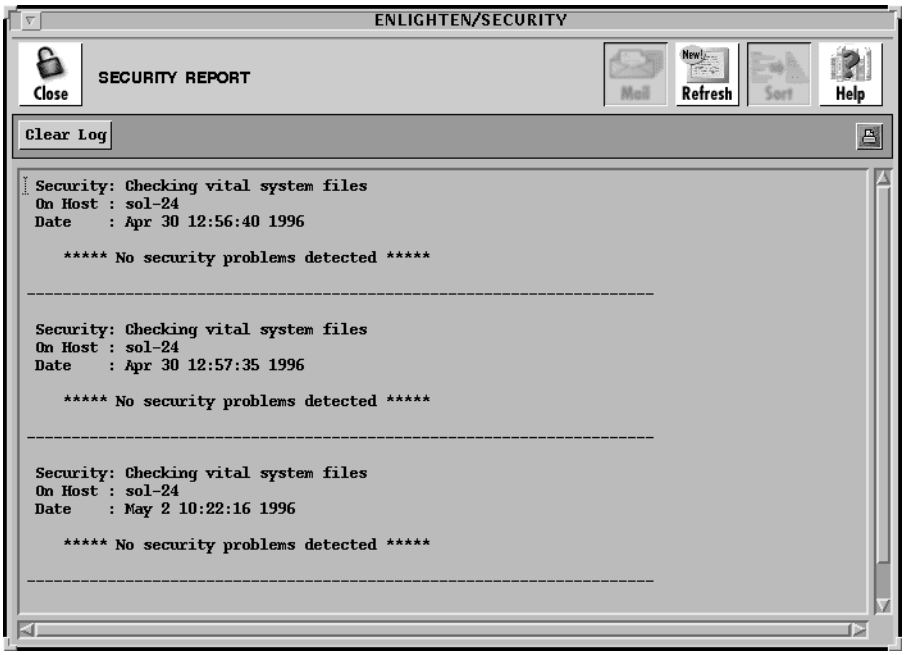

Figure 3-1 Security Logfile

Vital Files

This program will check the system directories and their files for easily breachable write permissions. It checks the following files and directories:

- `/etc`
- `/usr/adm`
- `/usr/bin`
- `/usr/etc`
- `/usr/lib`
- `/usr/local`
- `/usr/spool`

and creates a report listing any potential breaches it found.

File System Devices

This program will check that the raw device name of each mounted filesystem is in order. It looks at:

- The ownership of the device name (filesystem)
- The user group ownership of the device name (filesystem)
- Read and write permissions on the device name (filesystem)

and creates a report listing any potential problems it found.

Boot and Shutdown Script Checks

This program will check the contents of all files in the `/etc/rc*.d` directories and the `/etc/rc` files for potential back doors that could be activated at boot or shutdown time. These files are executed at boot time to initialize/shut down the system.

All the start-up and shutdown files referenced within the boot and shutdown scripts are checked for:

- The existence of the file
- Write permissions on the file
- Write permissions on the directory containing the file

and a report listing any problems found is then created. This process may be time-consuming when a large number of files is being checked.

Crontab Contents

This program will check the contents of the crontab files for potential back doors via the `cron` utility. All executable programs referenced in the cron tables are checked for:

- The existence of the file
- Write permission on the file
- Write permission on the directory containing the file
- crontab permissions on the file

and a report listing any problems found is then created.

Password File Integrity

This program will check the password file `/etc/passwd` for the following security breaches:

- No blank lines in the file
- Each entry has seven fields separated by colons (':')
- The username is alphanumeric
- The user has a password
- The Userid is numeric
- If the Userid is `0`, the login name is `root`
- The Groupid is numeric and exists in the group file
- The `HOME` directory of each entry exists
- The starting SHELL of each entry exists

and creates a report listing any problems it found.

Group File Integrity

This program checks the group file `/etc/group` for the following security breaches:

- No blank lines in the file
- Each entry has four fields separated by colons (':')
- The groupname is alphanumeric
- The GID is numeric
- The user group does not have a password
- Check each group member to see if:
  - The username is alphanumeric
  - They do not exist in duplicate within the group
  - They are valid users in the `/etc/passwd` file

and creates a report listing any problems it found.

User Home Directories

This program checks each user's HOME directory for the following potential problems:

- Make sure each user has a home directory
- Make sure the directory is *not* world writable
- Checks start-up scripts for world write permission
- Checks start-up scripts for group write permission

and creates a report listing any problems it found.

Attempted Break-ins

This program finds all the users who failed a second attempt to become superuser or some other user through the `su` command. It then creates a report listing any problems it found.

Obvious Passwords

One of the most frequent invasions of computer systems is not through a complex or back door trick, but through the front door via the login program. So, simple account passwords can be a high security risk.

Users frequently choose very simplistic passwords. While some systems have password programs to force some variation of simple passwords, the protection is usually minimal. You can use the Obvious Password security check to get a list of users with easily detectable passwords.

This program runs obvious password checks on:

- The user's login name
- The `passwd` file on the machine (hostname)
- All words in the user's Realname, Phone number, and Office user account fields of the `passwd` file

after you fill in the relevant data fields in the Password Check Parameters window (Figure 3-2).

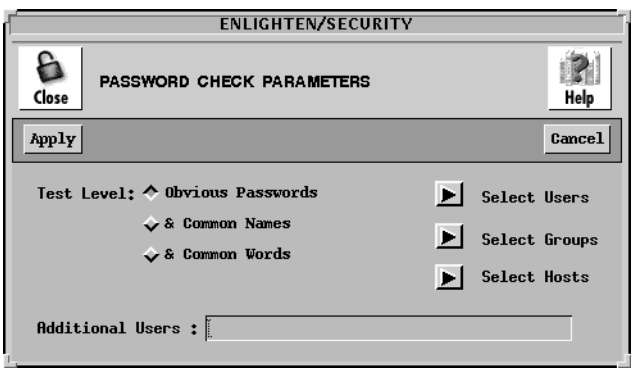

Figure 3-2 Password Check Parameters window

Since users have the ability to change their passwords at any time, you should run this security check frequently. Keeping a historical reference will also provide some insight into your own users' password habits.

Levels of Checking

There are three levels of Obvious Password Checking you can select, with level one being the lowest and each subsequent level encompassing the previous levels:

1) **Obvious Passwords**

   Passwords that closely match the account name. Each user takes approximately 5 seconds to check.

2) **Common Names**

   Passwords matching proper names, a frequent choice of novice users. Each user takes approximately 5 minutes to check.

3) **Common Words**

   Passwords found in a common-use dictionary. Each user takes approximately 30 minutes to check.

Who is Checked

Click the right arrows in the Password Check Parameters window for lists of the users, groups, and hosts on the system. You can use these to target specific users and/or groups for the checking process.

For the Users and Groups windows, you will be presented with the users and groups in the current system pool. Choosing a user or group will cause all occurrences of that user and/or group to be checked across the hosts in that system pool. For the Hosts window, selecting a host will check all users on that host.

Instead of using the above process, you may also choose to examine only specific targets by using the Additional Users field. Use the format `hostname:username` to specify these entries. The following example tests user *johnf* on host *rome* and all users on host *paris*.

Additional Users: `rome:johnf paris:`

Whichever method you use, when you are finished, click the Apply button. The time required to execute the testing process depends on the number of users to check and the level of checking. When this check is done, a list of users with obvious passwords appears in the form of the Configure Users window.

At this point, you could select a subset of the users and lock them out, obtain a list of their current processes, change their passwords, e-mail an "Obvious Password" letter to them, or even delete them.

What is Checked

All Options

ENlighten/DSM will check each word in the generated list of potentially obvious passwords as follows:

- As entered
- In all lowercase letters
- In all uppercase letters
- Capitalized first letter, the rest in lowercase.

Each of these checks will be performed on the actual word as well as its reverse. For example, 'Mirror' will be checked as Mirror, rorriM, mirror, rorrim, MIRROR, RORRIM.

This program will also check for accounts with no password, empty passwords and other obvious passwords such as "secret", "computer", "hello", etc.

The Common Names Option

The second level of password checking checks a list of 4000 names for possible matches. This list of names is found in the file `$ENLIGHTEN/config/names`. You may modify this file to fit your working environment.

Entries in the file are checked as is, from first to last, and any deviations such as capitalization or backwards spelling are not made. If you want these deviations to be checked, you need to add them sequentially as entries in the file.