System Administration
Week 10 Lab

April 17, 2006

1 Auditing Log Files

[**1**] Given the complexity of the root passwords of your accounts, you have probably failed to log in as root as least once. Look through the log files and see if you can find an entry for a fail login. If you haven't failed to log in at all, attempt to log into the system as root and type in the wrong password, and then find the corresponding log entry.

[**2**] Find the directory where Apache stores its log file and choose any entry in `access.log`. Can you guess the format of the log entry?

[**3**] As you read through the log entries, you'll notice that DHCP produces many useless entries. Using `grep`, can you figure out a way to filter DHCP entries from log files? Hint: You will probably need to use a pipe.

[**4**] After filtering out useless duplicate entries from your logs, what interesting entries can you find? Try to determine what they mean. To confirm your guesses, search the Internet for similar log entries and see if you can find out more information about the log entries.

2 Patching

[**1**] What series of commands would you execute to update all the packages on your system?

[**2**] Run these commands. Were there any updates to the packages you have installed on your system?

3 Automating Tasks

[**1**] Write a script to find all the files and directories with 777 permissions on your system. Can you think of any other insecure permissions? If so, add commands to find these types of files and directories on your system. Hint:

The man page for find contains a lot of information about the parameters you can use.

[2] Create a few files and directories with insecure permissions and see if your script locates them. If not, modify the syntax of the commands in your script so that it does.

You're going to add your script to your crontab. However, since your script produces output, you're going to have to tell the system where to send the output.

[3] Edit `/etc/aliases`. The format of the file is as follows:

```
username: email_address@domain.com, another@domain.com
```

Edit the file so that all mail sent to the user whose crontab you are editing is sent to your email address. Run `newaliases` to put the changes into effect.

[4] Add your script to crontab and set the time for it to execute within the next few minutes. Did you get an email with the list of the files and directories with insecure permissions?

4 Minimum User Access

[1] Determine the package name for `scponly` and install it.

[2] Add a new user to your system whose shell is `scponly`. Remember to provide the full path to `scponly` when creating the user account.

[3] Attempt to login as this new user using SSH. What happens? Are you able to execute any commands?

[4] Attempt to copy files to the account using `scp`. Does it work?

[5] Use `vipw` to change the shell of one your user accounts to `scponly`. Again, make to provide the full path to `scponly`. Can you login to the account using SSH? Can you perform any commands after logging into the account?