Lab Exercise
Operating Systems (Linux)

Treasure Hunt with “find”

Use the “find” command to search for the following files within the /usr directory of the Wary Puppy 5.3 file system.

1. Find a file called “newbieguide.html”, when was it last modified?
   (Hint: use the “-ls” switch to get more detail about each file or directory found.)

2. Apart from the file above which other file contains “guide” in the file name?

3. Find the file cpu.png, then find all the “.png” files in /usr/local that are newer than it.

4. Find all the index.html files, how many are there?

   a. Repeat the find command above but modify it so that the content of all the files is displayed.
      (Hint: use find, -exec and cat)

   b. Modify the command so that only the first 3 lines of each file are displayed.
      (Hint: use “head -3”)

   c. Repeat the find command above but modify it so that only lines in the found files containing the string “title” are displayed.

5. Find all files belonging to user “fido” note their name(s).

6. Find a file which has access permissions rwx r-x ---, note it’s name.

Answers are at the end of this document.

Word Search with GREP

grep filters its input based on string matching, this can be used to search for specific lines from a text file or to filter the output from another command.

grep uses regular expressions to specify the strings to be matched.

For experimenting with grep, it is useful to have a large file with many different string patterns to search. Luckily many computer file systems contain a large dictionary which is used for spell checking.

The Puppy Linux distribution has a dictionary with many thousand words, one per line, located at:-

/usr/share/myspell/dicts/en-US.dic

Navigate to the directory and use grep to search the word list for the following:-

1. Find a word which contains the text “linu”.

2. Find the name of a place which contains the text “cs” followed by an “n”.

3. What is the last word in the dictionary which contains the letters “c”, “s” and ”n” in order?

4. What is the first word in the dictionary which starts with “c” followed by “s” and then ”n”?
   (Hint: use “head” to see just the first line of output)

5. Find a word which starts with an “s” and contains every vowel character “aeiou” in order.

Answers are at the end of this document.

Basic Forensics

A web services company has reported suspected illegal activity on it’s company equipment. They run a small web server farm of 24 separate servers which should all be configured identically.

One of the servers is suspected of having been hacked and may have had it’s configuration altered remotely by a third party.

The company has provided you with copies of the (httpd.conf) configuration files from each of the 24 servers for forensic examination.

Your task is to identify which server has been altered and what changes the hacker has implemented.

The files are supplied in the file httpd.conf.tar.gz which is available in the File Repository using the PuppyLinux web browser.