Main Page

Minimize

Week 1B - Essential Grep

User: e0540252 e0540252 (GUEST)
e0540252@u.nus.edu
Registered Account
Log off Account Links
Machine State: **RUN**
Refresh in: 0:00.
Time left: 9 mins
Boot progress: complete

control **connect** *stats* *useful*

Home IP:	137.132.84.43
VM IP:	10.0.1.217
Direct:	telnet or ssh to linuxzoo.net
SSH:	unavailable
VM Web:	http://host-1-217.linuxzoo.net/
JScript Telnet:	Network / ~~Console~~
Java Telnet:	Auto
JavaScript SSH:	SSH
JavaScript VNC:	VNC
URI telnet:	linuxzoo.net
Connect:	Username: root, Password: secure

SHARED IP MODE

Essential Grep

A gentle introduction to searching through files and logs

To reset all the check buttons from a previous attempt click here

Question 1: using grep

Grep takes a minimum of 2 parameters. The first parameter is what you are looking for, and the second parameter is the file you are looking through. So to find all the lines containing "pendance" in /usr/share/dict/words you could say:

```
grep "pendanced" /usr/share/dict/words
```

Adapt this example to find all the words in `/usr/share/dict/words` and find the first word that contains the three letter sequence `wpa`
wpa word: pawpaw

Check Tests: Complete
Dictionary search PASSED

Question 2: count with grep

You can pass the output of grep directly into another command if you want to. This could allow you to nest searches (e.g. find all the words containing "wta" which end in "ing") or perform other sorts of processing. This is called piping, and the producer of the code goes on the left of the pipe

character and the processing command goes to the right. The pipe character is often in the bottom right of the keyboard, and look like "|" (do not confuse it with the colon ":");

The wc command when given the option "-l" (minus and the letter L in lower case) counts how many lines it has been given. So

```
grep "danced" /usr/share/dict/words | wc -l
```

finds all lines containing the string "danced" and gives it to wc for counting.

Use `grep` piped through `wc` on file /usr/share/dict/words to find the number of words that contain the letter x.
ber words: 2078

Check

Tests: Complete
x word count PASSED

Question 3: count with grep and save

You can save the output of a command to a file by ending the line with ">filename". So to save the number of lines to a file called "gordon" which contain "danced" in the dictionary you can do:

```
grep "danced" /usr/share/dict/words | wc -l > gordon
```

You can see file you have created using "ls" (a bit like "dir") and see the contents of a file using "cat" (e.g. cat gordon).

Use `grep` piped through `wc` on file /usr/share/dict/words to find the number of words that contain the letter x and save that answer to a file called "q1".

Check

Tests: Complete
x word count to file PASSED

Question 4: negative grep

The grep command can take various options or flags. These are specified at the start of the command using a "-" sign. One useful flag is the "negation" search, which looks for lines which do not match. This flag is "-v". So to look for how many words DO NOT have "danced" in them, and save that to a file stuff, you could do

```
grep -v "danced" /usr/share/dict/words | wc -l > stuff
```

Use `grep` to find all lines in `/etc/passwd` that do **not** have `nologin` one the line. Send the output to file `nolog`

Check

Tests: Complete
not nologin PASSED

Question 5: Download a log

Use the command wget to download one of my server's log files. You need to do:

```
wget http://linuxzoo.net/data/web.log -O log
```

This downloads one of my weblogs and saves it into a file called "log".

Check	Tests: Complete Downloaded ok PASSED

Question 6: Any 404

Look for file not found errors in this weblog. This is error 404. Although not a perfect method, you can do this by searching for " 404 " in the log. The spaces are important, otherwise a search for "404" would match "404hello" etc.

Once found save all of those to a file called "notfound".

Check	Tests: Complete Notfound lines PASSED

Question 7: The IP numbers

Process the "notfound" file and save a list of only the IP numbers of each log entry. This can be done using

```
cut -f1 -d" " filename
```

This gives the first "field" of the file "filename", where fields are delimited using the space " " character. Save that info to a file called "ip".

Check	Tests: Complete Just IPs PASSED

Question 8: Duplicates

If you "cat ip" you will see that there are many duplicate IPs shown. The "sort -u filename" command will sort uniquely that file and remove duplicates. It also sorts the entry alpha numerically. What is the last IP printed if this uniqueness processing is applied to the ip file?
Last Unique IP: 10.1.9.99

Check	Tests: Complete find .conf PASSED

Question 9: How many times

How many times does the above IP exist in the full log file "log"?
Count of Last Unique IP: 3

Check	Tests: Complete find new files PASSED

Centos 7 intro: Paths | BasicShell | Search

Linux tutorials: intro1 intro2 wildcard permission pipe vi essential admin net SELinux1 SELinux2 fwall DNS diag Apache1 Apache2 log Mail

Caine 10.0: Essentials | Basic | Search | Acquisition | SysIntro | grep | MBR | GPT | FAT | NTFS | FRMeta | FRTools | Browser | Mock Exam |

CPD: Cygwin | Paths | Files and head/tail | Find and regex | Sort | Log Analysis

Kali: 1a | 1b | 1c | 2 | 3 | 4a | 4b | 5 | 6 | 7a | 8a | 8b | 9 | 10 |

Useful: Quiz | Forums | Privacy Policy | Terms and Conditions

Site Links: XMLZoo ActiveSQL ProgZoo SQLZoo