Network Administration Homework 1

2012 Perl Scripts

Outline

- Part 1: Log parsing (40%+10%)
- Part 2: Plurk Bot (50%+10%)

Part 1: Log Parsing – (1)

- Write a perl program to parse log for ssh bruteforce
- Print the Users and times descending
- Syntax

  logparser.pl [-wur] [-h host | -n # | -t # -g filename] [file …]

  - -w mark the user exists in your system
  - -u sort by username
  - -r sort in reverse order
  - -h show only the user attack from the host
  - -n show only the user of the most #-th times
  - -t show only the # user of the most attacking times
  - -g output the graphic instead of text
  - files log file(s), if none, read from standard input
  - -? You can design any other fancy, fun(ny), or useful functionalitie

Part 1: Log Parsing – (2)

- SSH bruteforce log
  - Only parse these four (plus one) formats
    - Sep 1 15:46:39 NetAdm sshd[65884]: error: PAM: authentication error for illegal user yabc from
    - 140.113.235.102
    - Sep 1 17:56:58 NetAdm sshd[86323]: error: PAM: authentication error for illegal user pabcd from
    - 140.113.235.102
    - Sep 6 01:04:07 NetAdm sshd[28362]: error: PAM: authentication error for root from 60.29.39.243
    - Sep 6 01:04:08 NetAdm sshd[2874]: error: PAM: authentication error for root from 60.29.39.243
    - Sep 6 01:11:36 NetAdm sshd[71712]: Failed keyboard-interactive/pam for invalid user bart from
    - 60.29.39.243 port 1625 ssh2
    - Sep 6 01:11:39 NetAdm sshd[20535]: Failed keyboard-interactive/pam for invalid user bash from
    - 60.29.39.243 port 1782 ssh2
    - Sep 6 01:21:25 NetAdm last message repeated 21 times
    - Sep 9 00:06:55 NetAdm sshd[2726]: Invalid user edu29 from 140.127.112.188
    - Sep 9 00:06:55 NetAdm sshd[4556]: Invalid user edu04 from 140.127.112.188
    - Sep 9 00:06:55 NetAdm sshd[187]: Invalid user edu05 from 140.127.112.188

Part 1: Log Parsing – (3)

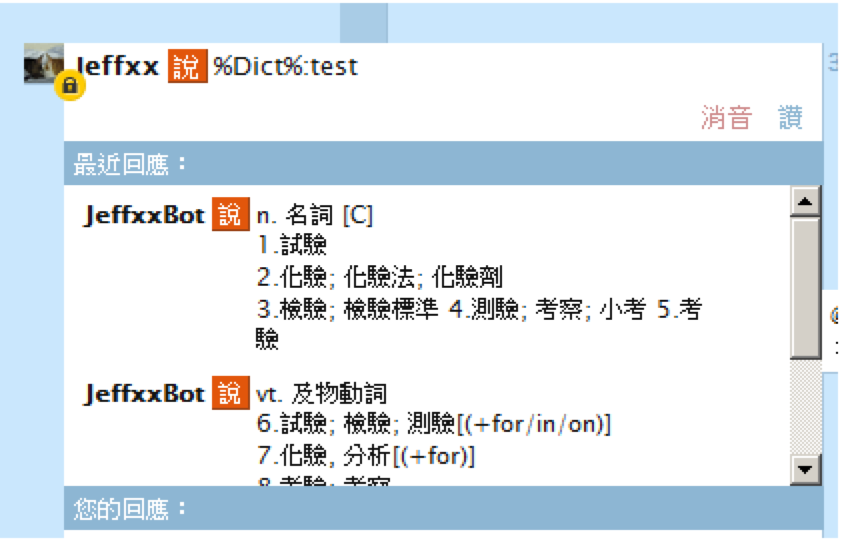
- Hints
  - Perl Regular Expression
  - Hash
  - Sorting
  - p5-GD
  - Getopt::Std
  - …

Part 2: Plurk Bot

- Bot must reply the msg beginning with
  - %Dict%: string
  - %Find%: userid,keyword
- %Dict%: apple
  - Reply the meaning of “apple” in Chinese
- %Find%: userid,apple
  - Reply the url of jeffxx's talks that contain 'apple'

Part 2: Plurk Bot – (2)

- %Dict%:
  - Use ydict’s output to reply
  - Only show chinese , no english
  - Reply Each type



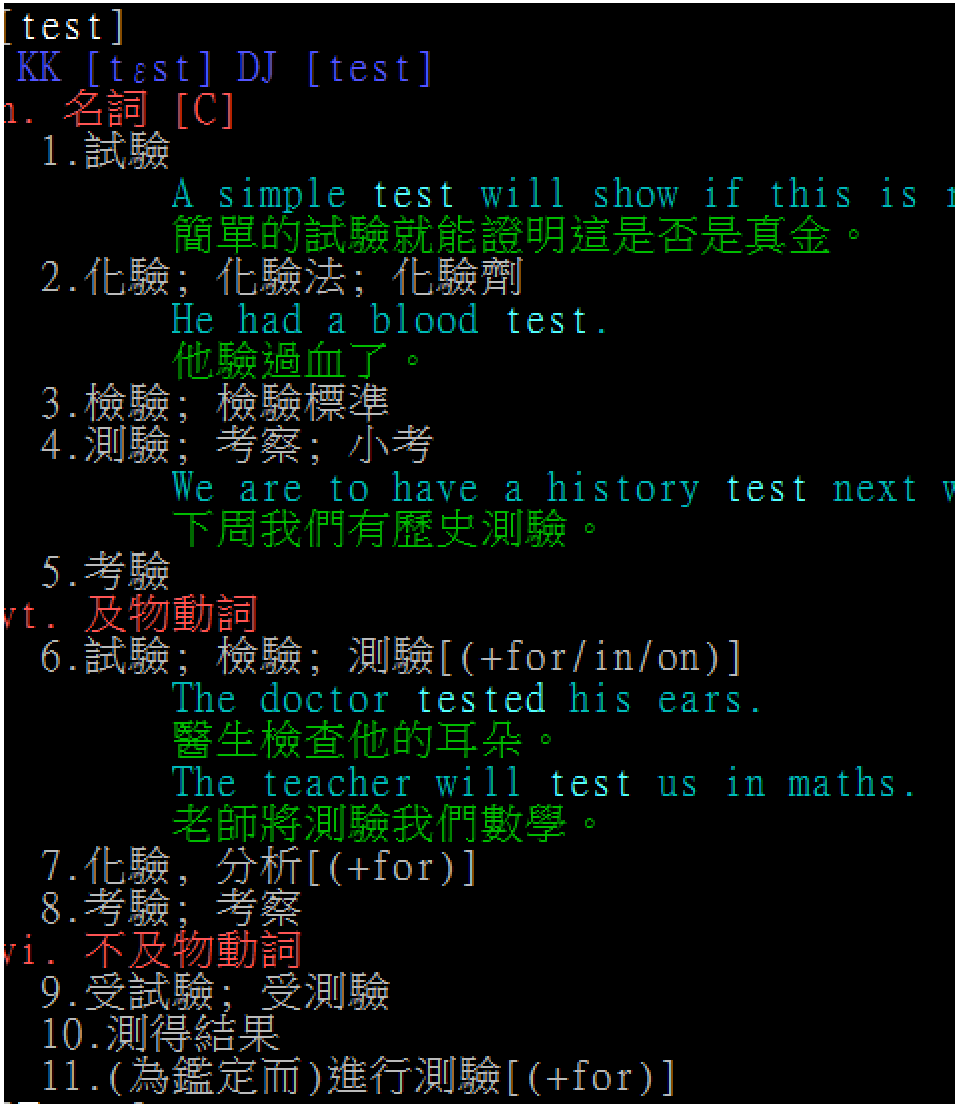
Jeffxx 說 %Dict%:test

最近回應：

JeffxxBot 說 n. 名詞 [C]
1.試驗
2.化驗; 化驗法; 化驗劑
3.檢驗; 檢驗標準 4.測驗; 考察; 小考 5.考驗

JeffxxBot 說 vt. 及物動詞
6.試驗; 檢驗; 測驗[(+for/in/on)]
7.化驗, 分析[(+for)]
8.考驗; 考察

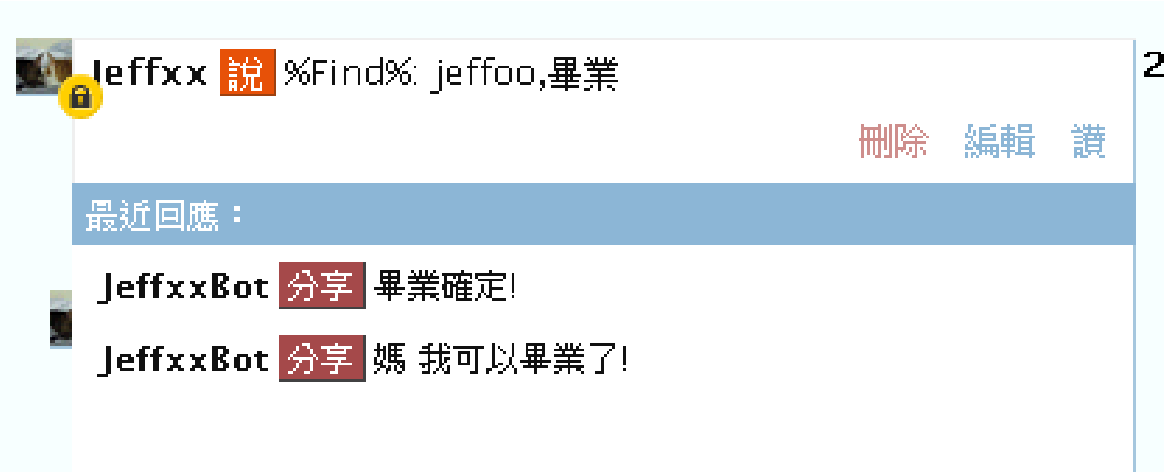
您的回應：



```
[test]
 KK [tεst] DJ [test]
n. 名詞 [C]
  1.試驗
        A simple test will show if this is r
        簡單的試驗就能證明這是否是真金。
  2.化驗; 化驗法; 化驗劑
        He had a blood test.
        他驗過血了。
  3.檢驗; 檢驗標準
  4.測驗; 考察; 小考
        We are to have a history test next w
        下周我們有歷史測驗。
  5.考驗
vt. 及物動詞
  6.試驗; 檢驗; 測驗[(+for/in/on)]
        The doctor tested his ears.
        醫生檢查他的耳朵。
        The teacher will test us in maths.
        老師將測驗我們數學。
  7.化驗, 分析[(+for)]
  8.考驗; 考察
vi. 不及物動詞
  9.受試驗; 受測驗
  10.測得結果
  11.(為鑑定而)進行測驗[(+for)]
```

Part 2: Plurk Bot – (3)

- %Find%:
  - Search the user’s timeline ,reply the message containing keyword.
  - Only Need Search 50 Public plurks .



Jeffxx 說 %Find%: jeffoo,畢業

JeffxxBot 分享 畢業確定!

JeffxxBot 分享 媽 我可以畢業了!

Part 2: Plurk Bot – (4)

- Something Useful
  - http://www.plurk.com/API
  - http://blog.urdada.net/2011/10/28/426/
  - /usr/ports/chinese/ydict
  - …