Corso di Sistemi Operativi e Reti

Prova scritta telematica 30 LUGLIO 2020

ESERCIZIO 1, TURNO 1 - PERL

Si scriva uno script Perl dal nome `analyzer.pl` che esegua le seguenti operazioni.
Lo script riceve come argomenti da linea di comando il `path/ad/un/file` di log relativo agli accessi ssh ad una determinata macchina Linux.

Il file di log, al suo interno, contiene righe di questo tipo:

- `Jul 19 06:33:15 cisco sshd[27387]: Invalid user admin from 113.31.118.201 port 60784`
- `Jul 19 06:33:18 cisco sshd[21387]: Failed password for invalid user admin from 97.35.1.78 port 35767 ssh2`
- `Jul 20 10:32:10 cisco sshd[29704]: Accepted password for francesco from 151.81.167.39 port 50722 ssh2`

Lo script dovrà stampare su `FILE` e per ogni **utente** il cui tentativo di accesso risulta essere **invalido**, il **numero di tentativi** effettuati seguito dalla **lista di tutti gli indirizzi `IP` e `PORTA`** tramite cui si è tentato l'accesso. **La stampa dovrà essere ordinata per numero decrescente di tentativi e, a parità di numero di tentativi dell'utente, in ordine lessicografico di utente.**

N.B.: Un tentativo di accesso risulta essere fallito se la riga corrente del file contiene (in un qualsiasi punto) la stringa `Invalid user utente from x.x.x.x port 12345` dove **utente, ip** e **porta** possono variare.

Esempio (breve). Vedere pagine successive per un esempio completo

Nel caso del breve esempio di cui sopra, l'output dovrà essere il seguente:

admin 2
113.31.118.201:60784
97.35.1.78:35767

Importante:

1. Tutti i match sulle stringhe devono essere effettuati tramite opportuna REGEXP case insensitive.
2. Il file dovrà essere letto eseguendo, tramite chiamata Perl, il comando shell esterno atto a visualizzarne il contenuto
3. La stampa su file dovrà essere effettuata tramite funzione del linguaggio Perl.

 # Esempio (output ottenuto da un reale file auth.log)

```
admin       76
      113.31.118.201:60784
      14.33.45.230:45844
      14.33.45.230:45844
      ...

test        50
      113.31.118.201:53264
      113.31.118.201:53264
      ...

ubuntu      28
      13.127.216.186:48272
      191.252.0.25:37088
      ...

postgres    24
      113.31.118.201:45938
      191.252.0.25:34190
      ...

mysql       20
      113.31.118.201:51110
      113.31.118.201:51110
      ...
```

CONTENUTO DEL FILE auth.log

```
Jul 19 06:33:15 cisco sshd[27387]: Invalid user admin from 113.31.118.201 port 60784
Jul 19 06:33:16 cisco sshd[27387]: pam_unix(sshd:auth): check pass; user unknown
Jul 19 06:33:16 cisco sshd[27387]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=113.31.118.201
Jul 19 06:33:18 cisco sshd[27387]: Failed password for invalid user admin from 113.31.118.201 port 60784 ssh2
Jul 19 06:33:18 cisco sshd[27387]: Received disconnect from 113.31.118.201 port 60784:11: Bye Bye [preauth]
Jul 19 06:33:18 cisco sshd[27387]: Disconnected from invalid user admin 113.31.118.201 port 60784 [preauth]
Jul 19 06:36:47 cisco sshd[27389]: Invalid user zabbix from 113.31.118.201 port 34640
Jul 19 06:36:47 cisco sshd[27389]: pam_unix(sshd:auth): check pass; user unknown
Jul 19 06:36:47 cisco sshd[27389]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=113.31.118.201
Jul 19 06:36:49 cisco sshd[27389]: Failed password for invalid user zabbix from 113.31.118.201 port 34640 ssh2
Jul 19 06:36:49 cisco sshd[27389]: Received disconnect from 113.31.118.201 port 34640:11: Bye Bye [preauth]
Jul 19 06:36:49 cisco sshd[27389]: Disconnected from invalid user zabbix 113.31.118.201 port 34640 [preauth]
Jul 19 06:40:16 cisco sshd[27392]: Invalid user paula from 113.31.118.201 port 36466
Jul 19 06:40:17 cisco sshd[27392]: pam_unix(sshd:auth): check pass; user unknown
Jul 19 06:40:17 cisco sshd[27392]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=113.31.118.201
Jul 19 06:40:18 cisco sshd[27392]: Failed password for invalid user paula from 113.31.118.201 port 36466 ssh2
Jul 19 06:40:19 cisco sshd[27392]: Received disconnect from 113.31.118.201 port 36466:11: Bye Bye [preauth]
Jul 19 06:40:19 cisco sshd[27392]: Disconnected from invalid user paula 113.31.118.201 port 36466 [preauth]
Jul 19 06:43:40 cisco sshd[27394]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=113.31.118.201  user=backup
... ALTRE RIGHE ...
```