ESERCIZIO TRATTO DALLA PROVA D'ESAME DI SETTEMBRE 2019

Si scriva uno script `PERL` dal nome `auth.pl` in grado di fornire analisi dettagliate riguardanti eventuali accessi non autorizzati registrati nel file `auth.log` di Linux. Il file si compone di più righe del seguente tipo:

Sep 2 06:25:12 server sshd[15334]: Failed password for invalid user lyssa from 103.228.55.79 port 45462 ssh2
Sep 2 06:25:12 server sshd[15334]: Received disconnect from 103.228.55.79 port 45462:11: Bye Bye [preauth]
Sep 2 06:25:12 server sshd[15334]: Disconnected from invalid user lyssa 103.228.55.79 port 45462 [preauth]
Sep 2 06:25:16 server sshd[15336]: Invalid user test from 45.55.35.40 port 33438
Sep 2 06:25:16 server sshd[15336]: pam_unix(sshd:auth): check pass; user unknown
Sep 2 06:25:16 server sshd[15336]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=45.55.35.40

Come è possibile notare, la prima riga è composta dalla data e dall'ora in cui si è verificato il tentativo di connessione (**Sep 2 06:25:12**) succeduta da altri parametri e dalla stringa **"Failed password for invalid user"** seguita dal nome utente che ha tentato la connessione (nell'esempio **lyssa**), dall'indirizzo IP dal quale è provenuta la connessione (nell'esempio **103.228.55.79**) ed infine dalla porta sorgente (nel caso in esame **45462**).

Di seguito è riportata la sinossi del comando da implementare

```
./auth.pl [-ip|-user username] nome_file
```

Lo script, a seconda dell'opzione inserita in fase di esecuzione, eseguirà una tra seguenti operazioni:

1. **`./auth.pl -ip nome_file`** : lo script legge il file di accesso il cui nome viene passato su linea di comando tramite il parametro `nome_file`; per ogni riga contenente la stringa **"Failed password for invalid user",** salva l'indirizzo IP sorgente in una apposita struttura dati e, per ogni IP riscontrato, conta i tentativi di connessione non autorizzati provenienti dallo stesso indirizzo (ovvero le occorrenze dello stesso indirizzo IP nelle righe contenenti la stringa **"Failed password for invalid user"**). Lo script termina stampando su STDOUT la coppia `IP - NUMERO_OCCORRENZE` in ordine **decrescente**.
2. **`./auth.pl -user utente nome_file`** : lo script legge il file di accessi il cui nome viene passato da linea di comando tramite il parametro `nome_file`; per ogni riga contenente la stringa **"Failed password for invalid user"** conta gli accessi effettuati dallo user dal nome `utente` e memorizza tutte le date in cui tale utente ha effettuato i tentativi di accesso. Lo script termina stampando su file la coppia `NOME_UTENTE - NUMERO_ACCESSI` nella prima riga del file, seguita da **`N`** righe contenenti le date in cui si è tentato l'accesso.