GRAYLOG Search

Notebook: Tap nham
Created: 01/26/15 1:11 PM **Updated:** 02/11/19 3:23 PM
URL: https://github.com/hocchudong/ghichep-graylog/tree/master/graylog2

404 NOT FOUND cho NGINX va APACHE

(apache OR nginx) AND http_response_code:404

SAI USER TRONG SSH

"Failed password for invalid user"

LOC RA USER DANG NHAP TRONG DASHBOARD OPENSTACK

http://prntscr.com/5x79i3

Lọc ra địa chỉ IP Nguồn truy cập vào WEB

http://prntscr.com/5x7zoy

^*(.+) - -\B

SSH THẤT BẠI (tất cả các user)

application_name:sshd AND message:"Failed password for"

hoặc

application_name:sshd AND message:" pam_unix(sshd:auth): authentication failure "

SSH THÀNH CÔNG

application_name:sshd AND message:" pam_unix(sshd:auth): authentication failure "

SSH từ IP

- Bản tin 1: Failed password for invalid user sfd from 203.162.130.241 port 7177 ssh2
- Bản tin 2: Accepted password for uvdc from 203.162.130.241 port 11036 ssh2

^.*user (.+) from\b

HTTP

LẤY CODE TRONG HTTP

```
^.*HTTP/1.1" (.+?)\s\b
```

Tìm kiếm tổng số user đang nhập sai

```
application_name:sshd AND (message:"Accepted password for" OR message
:" pam_unix(sshd:auth): authentication failure ")
```

Regex lấy ra user sai

http://prntscr.com/c6quwy

Bản tin:

```
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
tty=ssh ruser= rhost=221.194.44.219 user=root
```

Các tìm kiếm

```
^.*user=(.+)$
```

LOG USER SSH

I put together some example regex to match the fields you listed.

ssh username

```
\w+ \d{2} \d{2}:\d{2}:\d{2} \w+ sshd\[\d+\]: .*? user (\w+) from
```

ssh source_ip

```
\w+ \d{2} \d{2}:\d{2}:\d{2} \w+ sshd\[\d+\]: .*? user \w+ from \b([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})\b
```