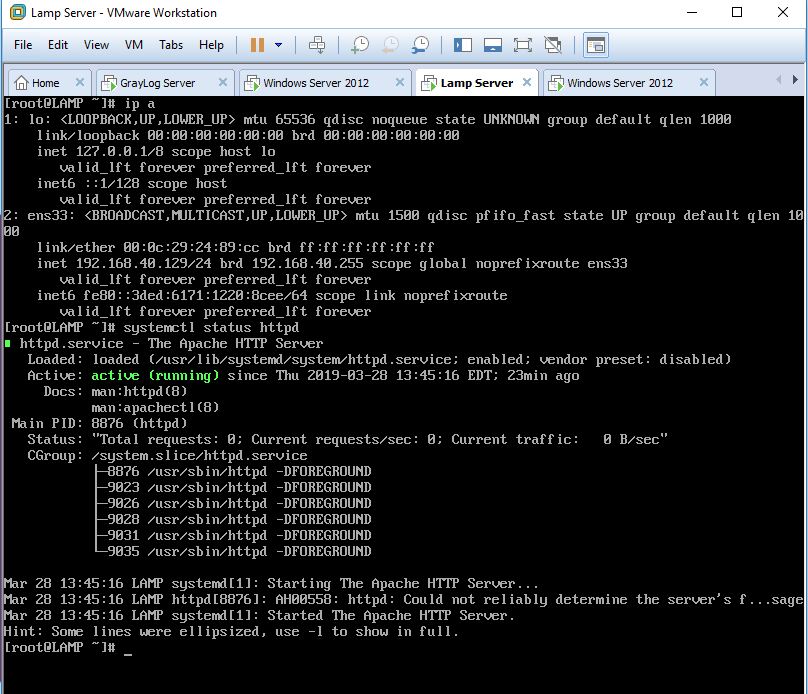
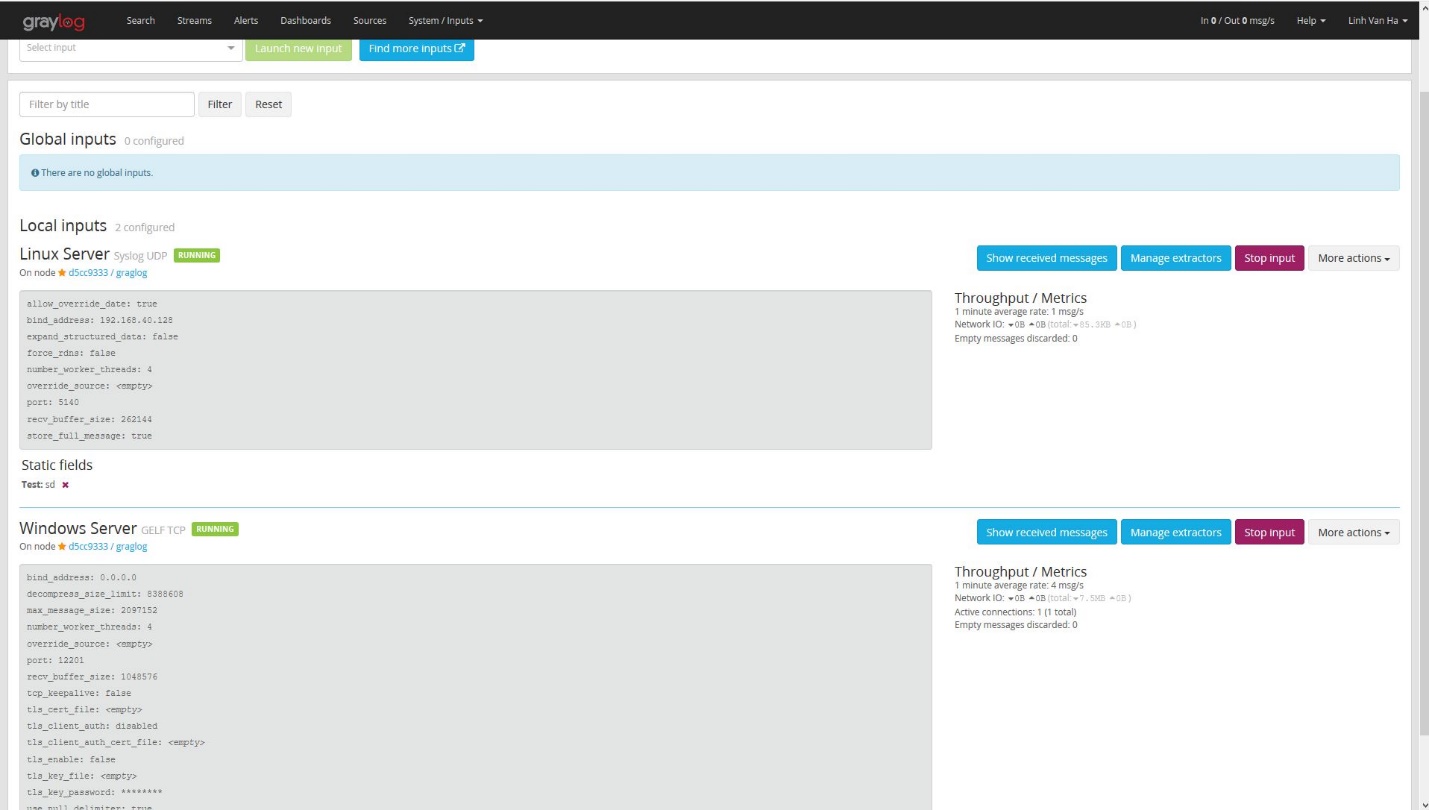
**Assignment: Centralized Logging**

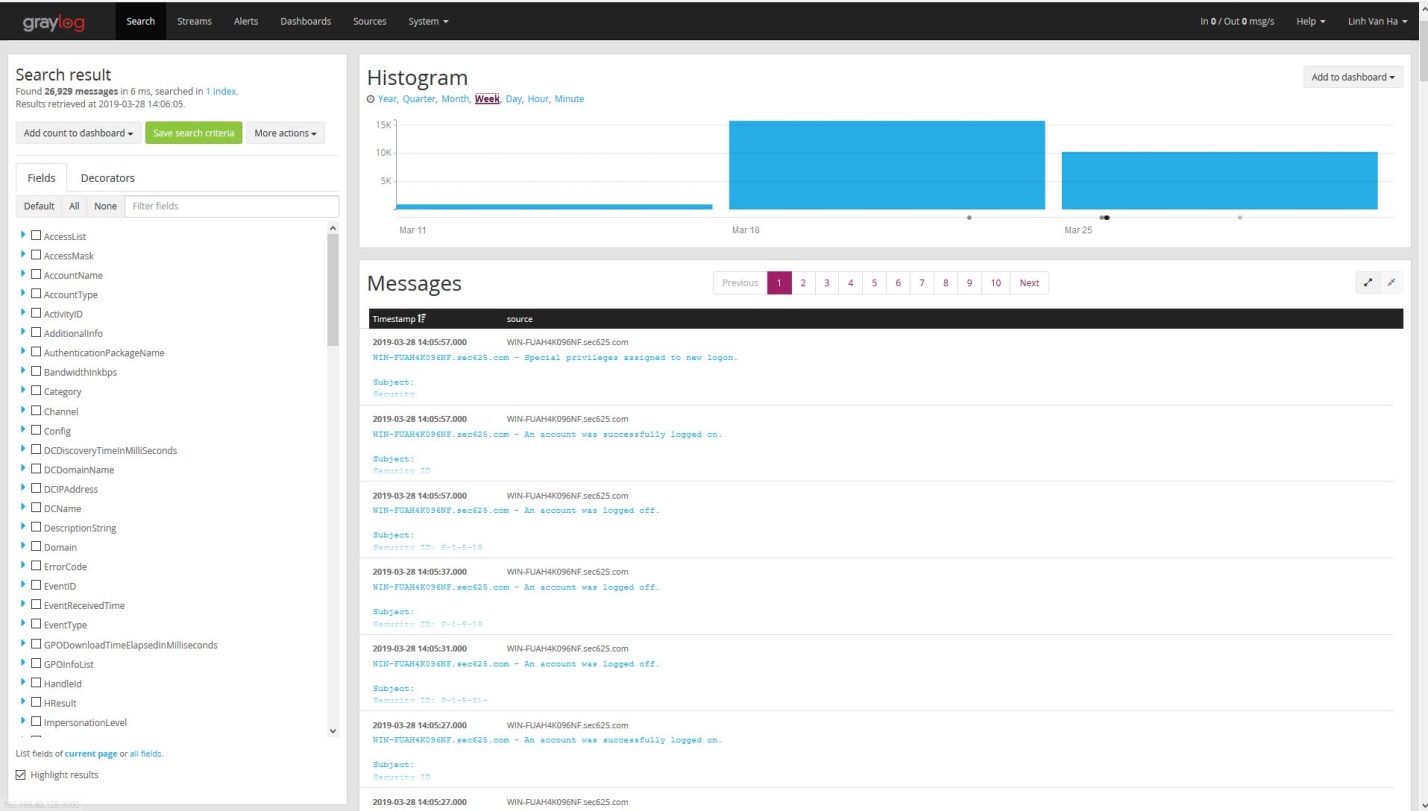
***Lab Report Submission***

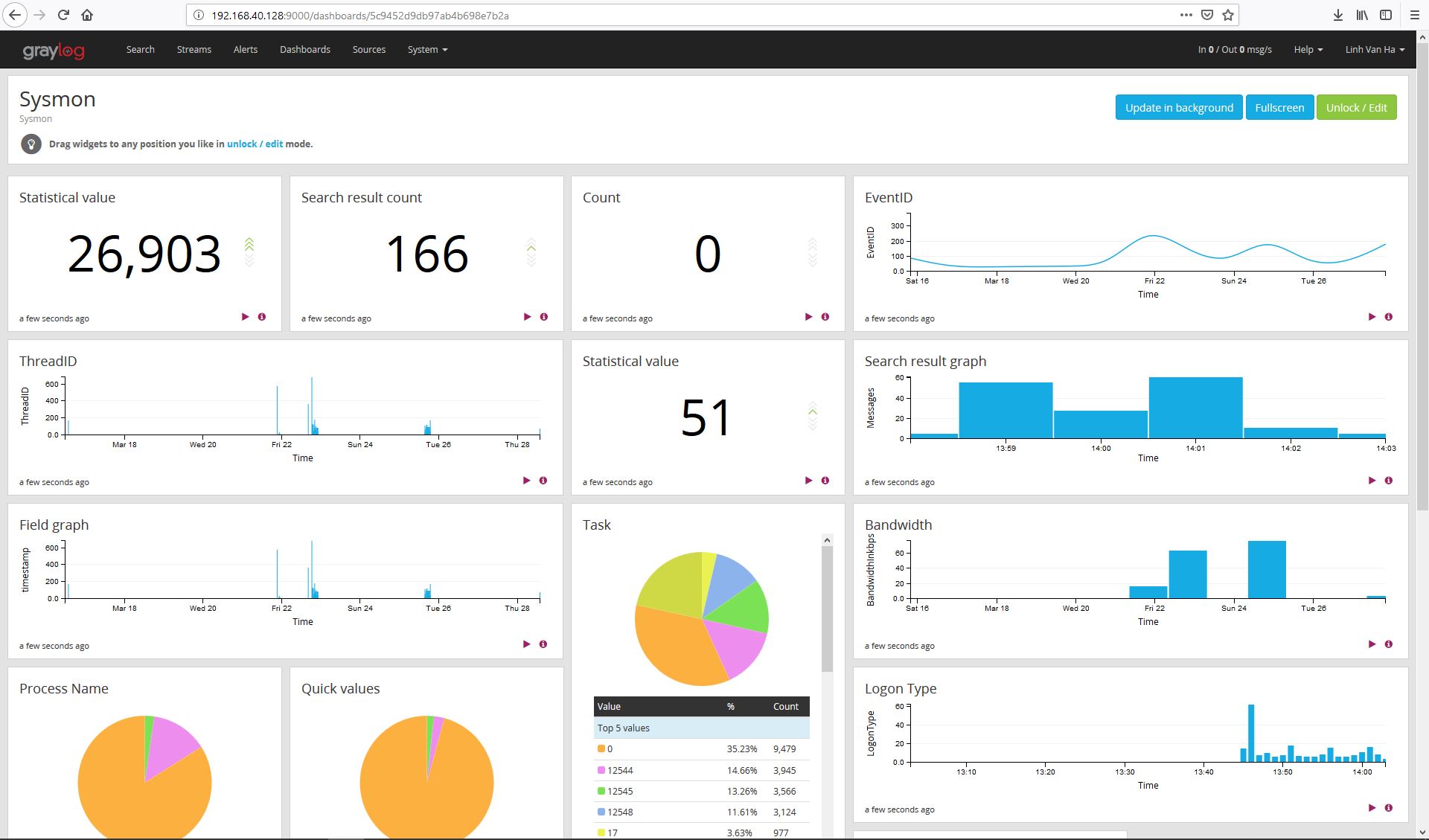
**Name: Winston Lam (156576175), Linh Van Ha (116592171) and Mohamed Yusuf (118058171)**

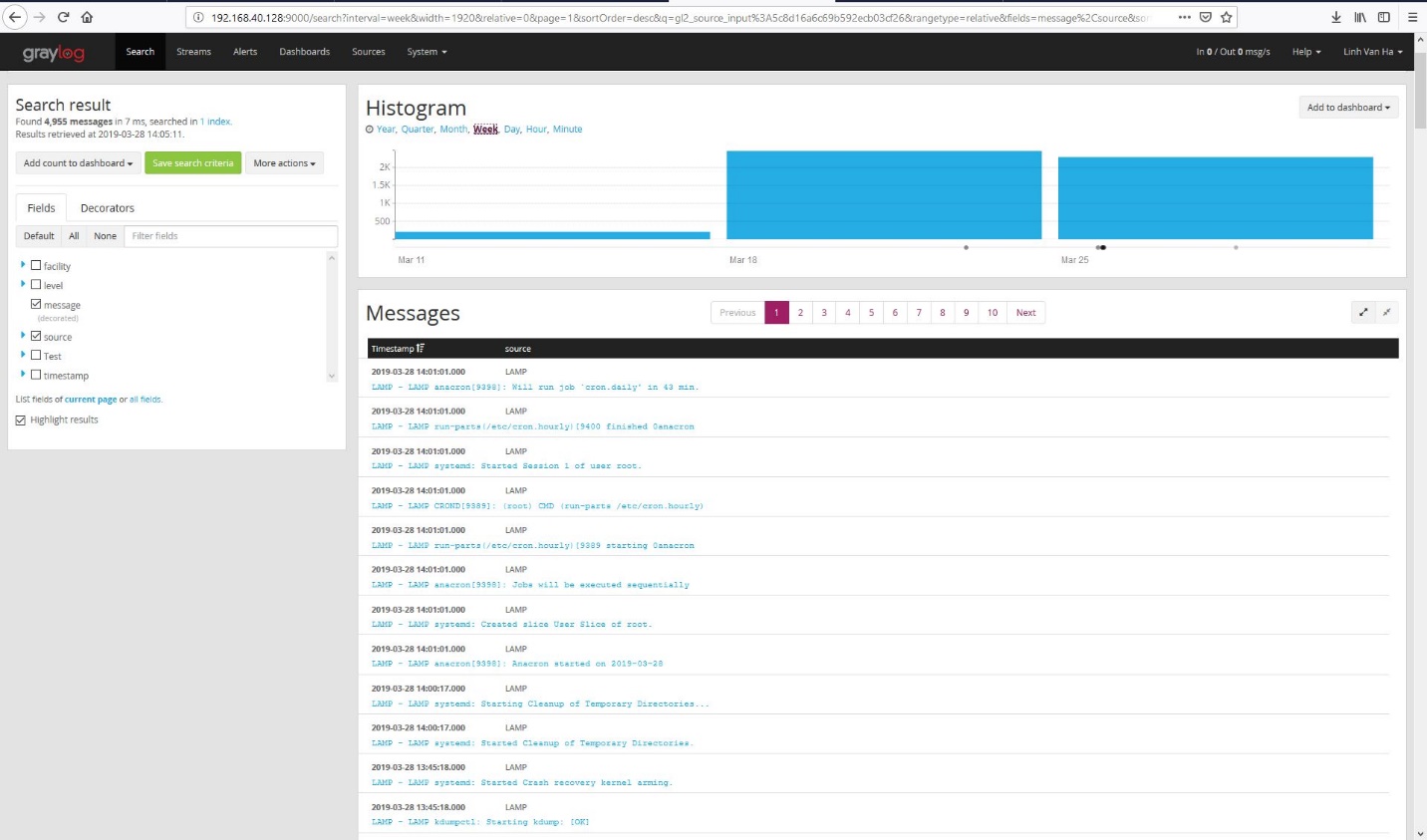
**Screenshot of LAMP**

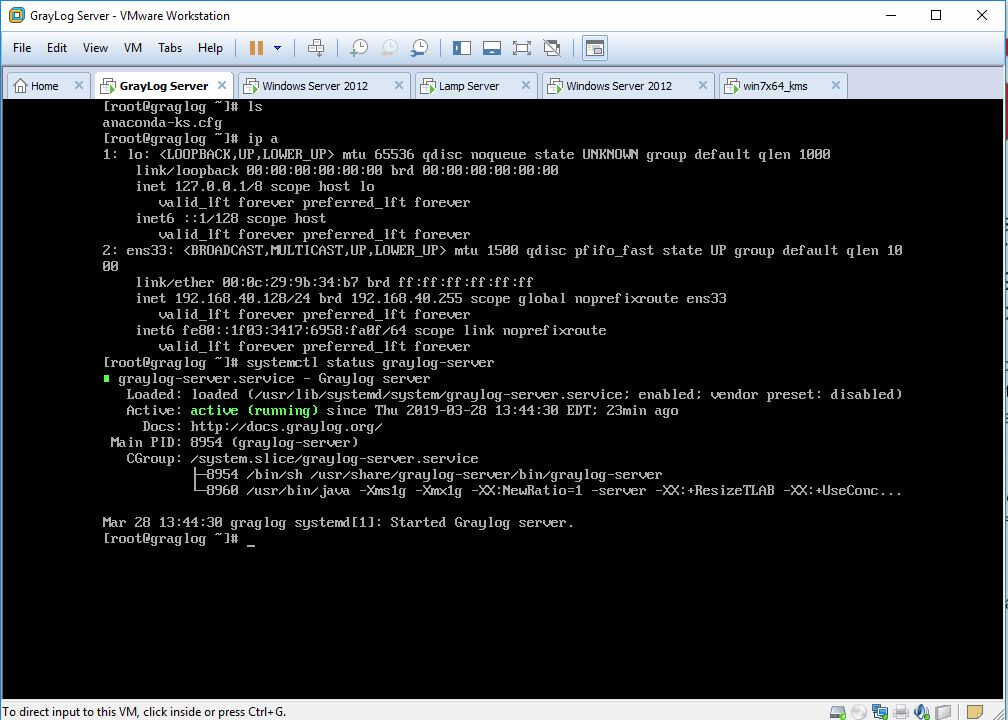
**Screenshot of GrayLog**

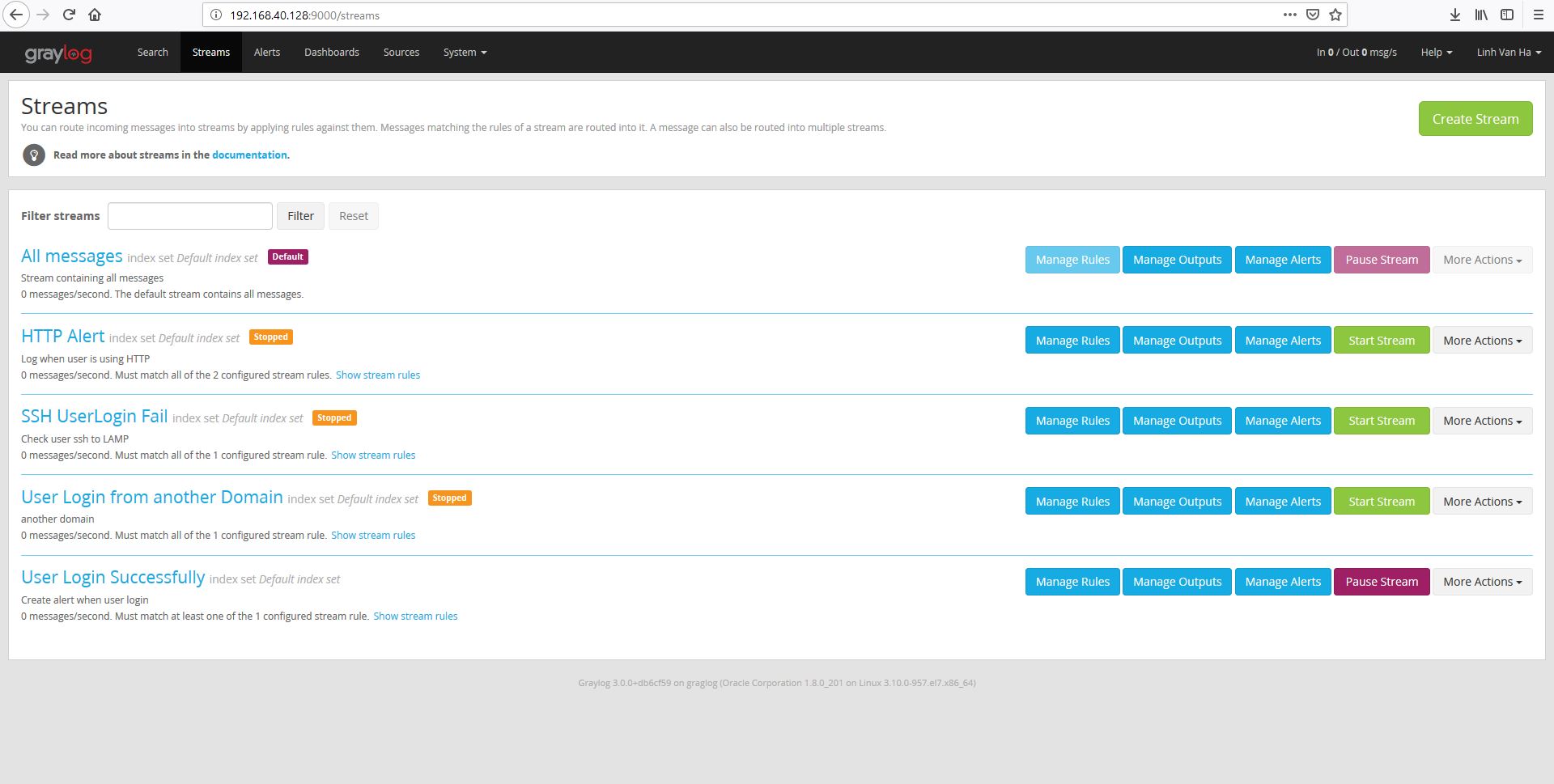
****

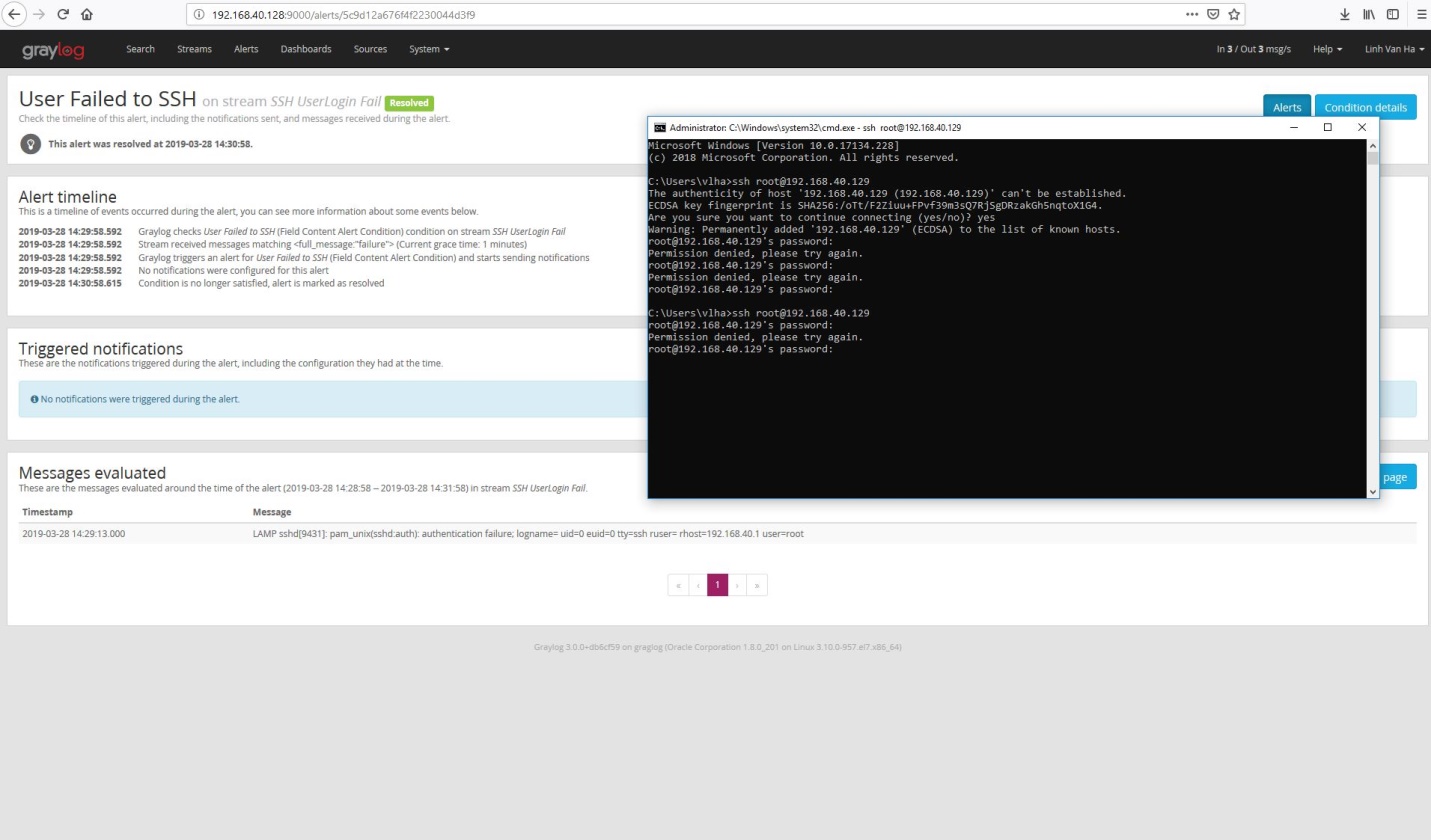
****

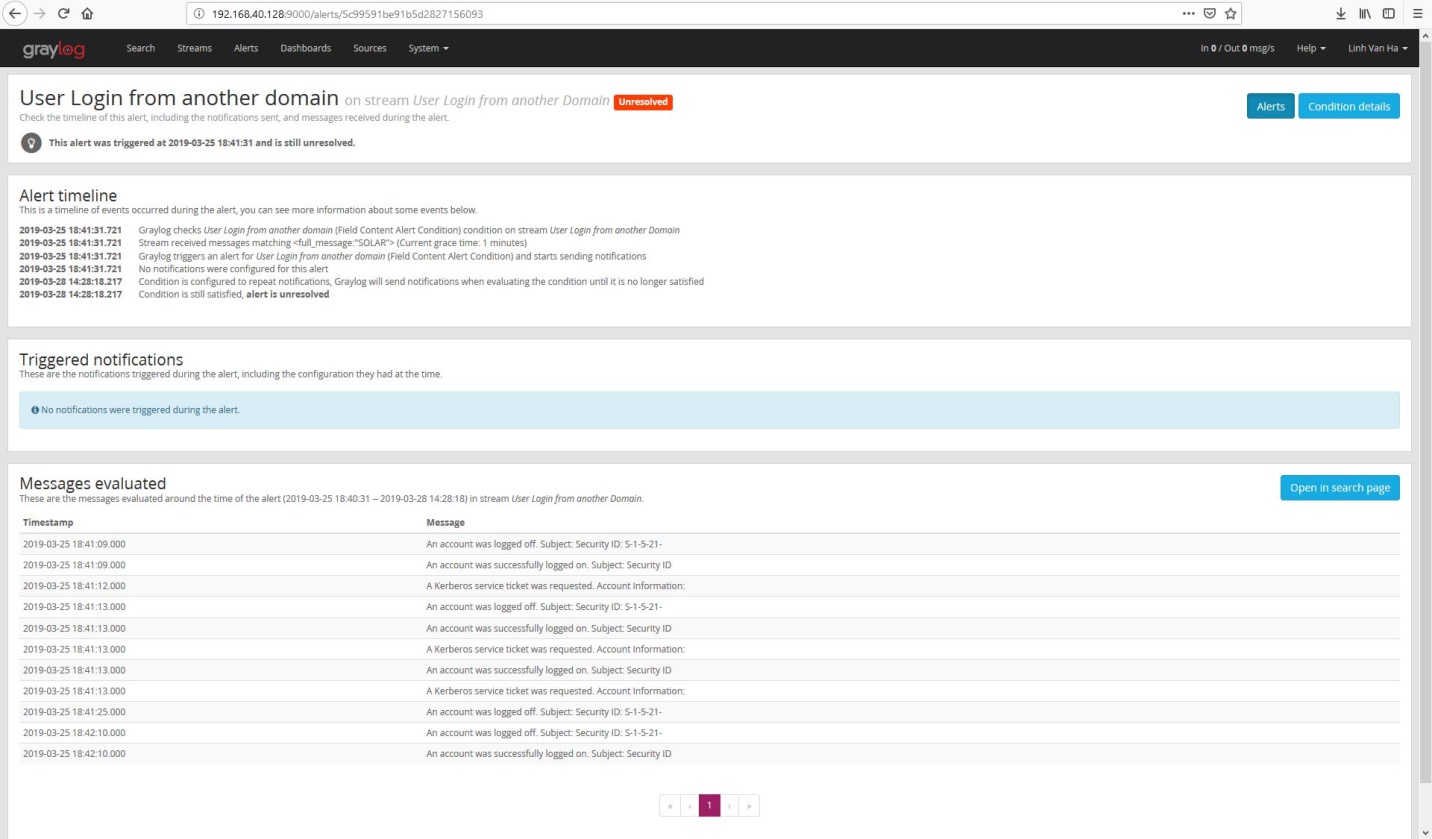
****

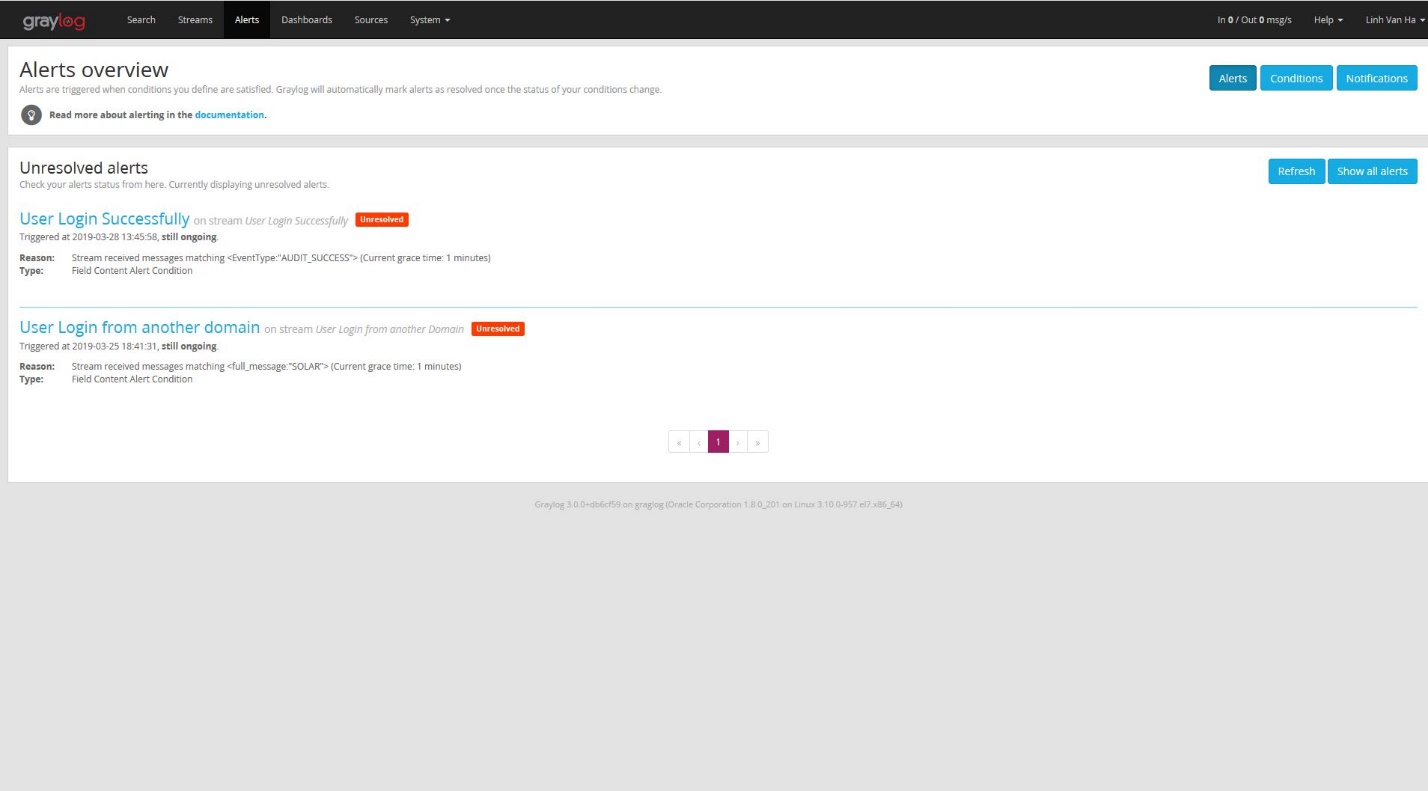
****



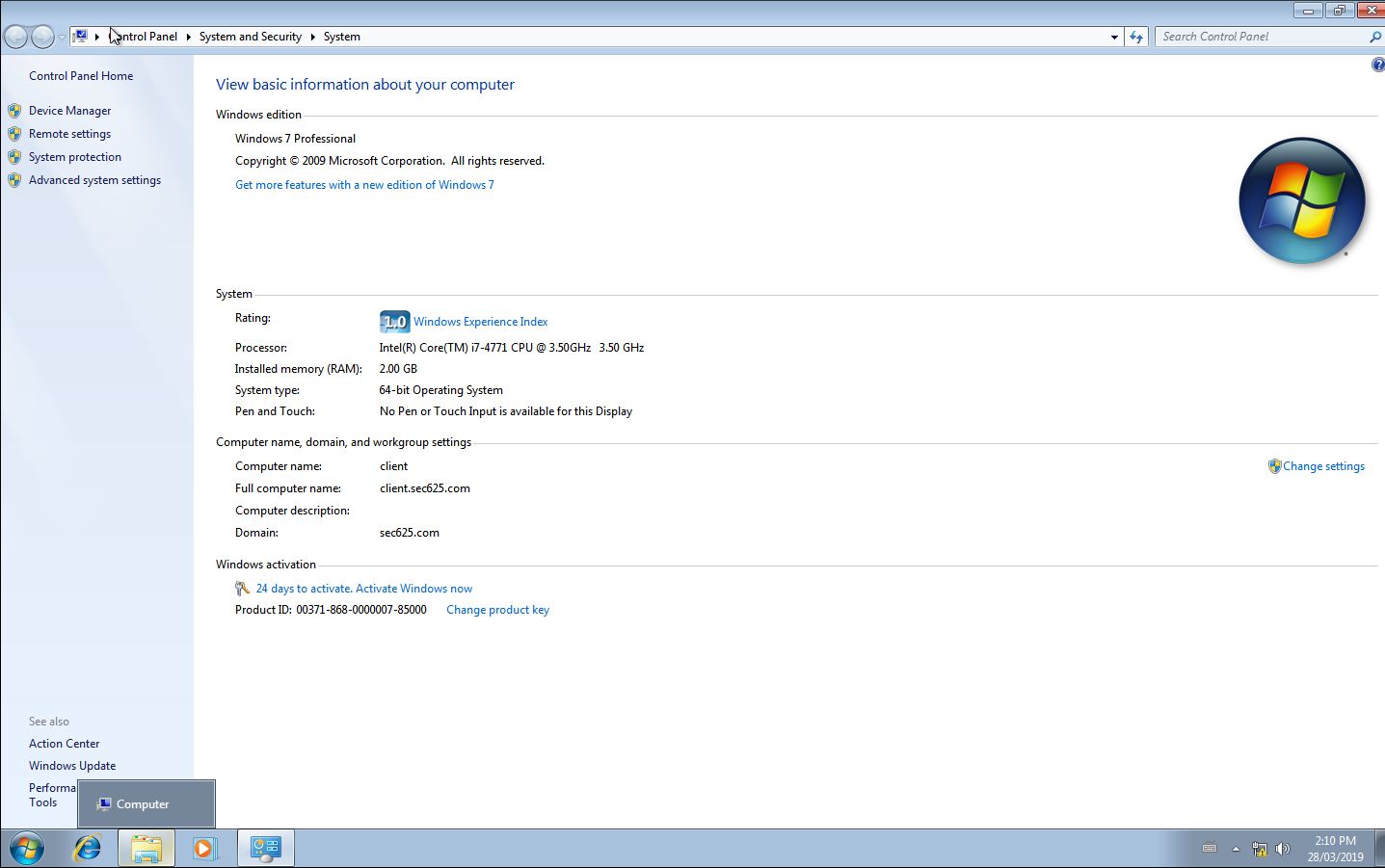








**Screenshot of Windows 7**



**Graylog**

One of the events that trigger security alerts on Graylog is “Field Content Alert Condition”. Under this condition, it will be triggered whenever the stream receives 1 and more messages since the previous alert run that has a field set to a particular value. Another event is, “Field Aggregation Alert System”. This event is triggered when the result of a statistical calculation of a numerical field is higher/lower than the actual threshold. The last event is “Message Count Alert Condition”. This event is triggered when we receive more messages in the last “X” amount of minute.

**Process of Graylog**

The Graylog Server collects log from Windows Server and LAMP server by using nxlog and rsyslog. All of the events from the system will be transferred and sent to Graylog Server. Administrators can make a stream and trigger the alert by making a rule in the log that they want to define. Every time the system catches a log that matches the condition of the rule, the graylog server will trigger the alert and will then notify the administrator instantly. The notification can in a form of email or directing it to the preconfigured website.

**Windows Server**

The event that triggers security alerts on Windows Server is “User login from another domain”. Users from the same forest attempting to login from another domain, the server will automatically save the log. This will trigger the alert to warn the administrator that the user from another site is attempting to use the network resources.

**Linux LAMP server – SSH login:**

There are always risks when it comes to transmitting any form of data across any network. It is important to encrypt all data with a strong password. A strong password should have at least 6 characters with a mix of letters, numbers and symbols. As well, restrict users from using their previous passwords and lock user accounts after numerous attempts of attempting to log in. With lots of users, it is important to collect information on their activities and analyze them for a potential risk. Using tools such as “psacct” can help monitor their activities on a continuous basis.

To add on, it is best to have a security banner with some form of security warning before the user is required to authenticate their credentials. This can help protect their SSH logins to unauthorized users. Most importantly, while using the Linux server, never login as root unless it we are required to do so. Disabling root login and allowing only specific users to access root is the most secure way. External users will try to access root accounts through SSH attacks by using different account names and passwords. Within most network configurations, usernames, passwords and transferred files can be taken from anyone who is on the same network as you. They use something called a “packet sniffer” which targets packets that are transmitted over the internet.

**References**

40 Linux Server Hardening Security Tips [2019 edition]. (2019, March 19). Retrieved March 28, 2019, from https://www.cyberciti.biz/tips/linux-security.html

Alerts. (n.d.). Retrieved September 3, 2019, from http://docs.graylog.org/en/2.4/pages/streams/alerts.html

Brandall, B. (2018, March 21). 34 Linux Server Security Tips & Checklists for Sysadmins | Process Street | Checklist, Workflow and SOP Software. Retrieved March 28, 2019, from https://www.process.st/server-security/

Saive, R. (2012, December 14). 5 Best Practices to Secure and Protect SSH Server. Retrieved March 28, 2019, from https://www.tecmint.com/5-best-practices-to-secure-and-protect- ssh-server/

Saive, R. (2015, January 3). 25 Hardening Security Tips for Linux Servers. Retrieved March 28, 2019, from https://www.tecmint.com/linux-server-hardening-security-tips/