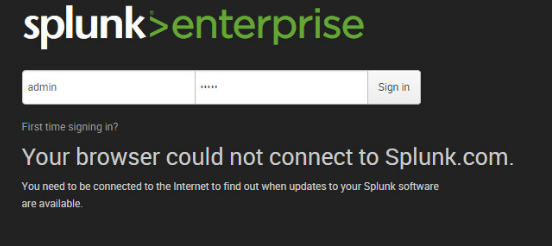
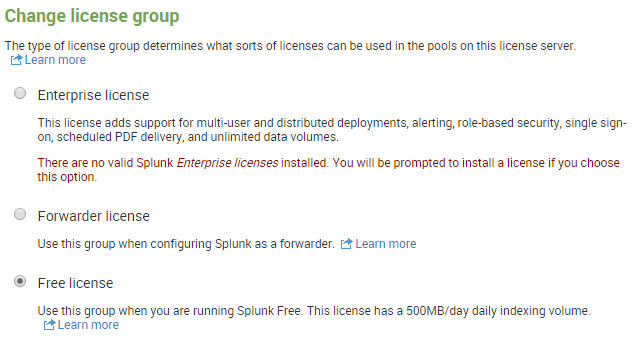
Splunk

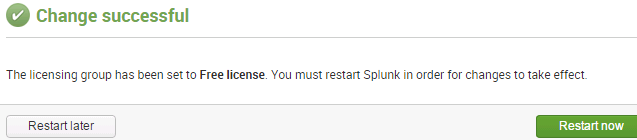
Splunk is a SIEM (Security Information and Event Management) solution that uses big data from websites, applications, servers, networks, sensors, and mobile devices for more efficient analysis. It is particularly useful for event correlation and supports a wide variety of environments.

Splunk setup :

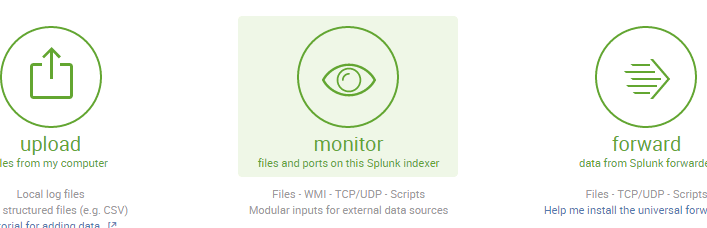


License selection Screen (Free License)

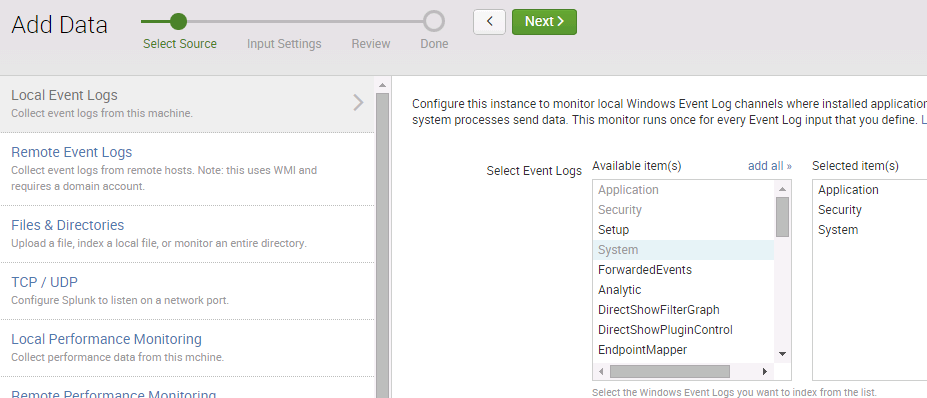




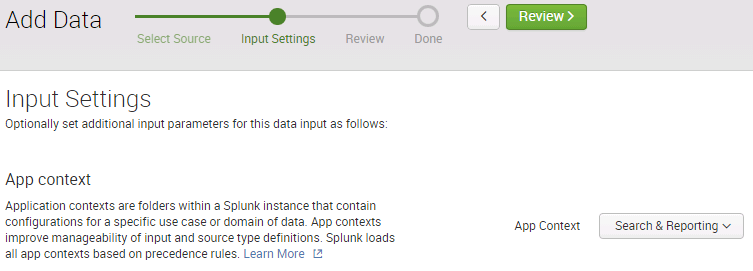
Adding data > Monitor

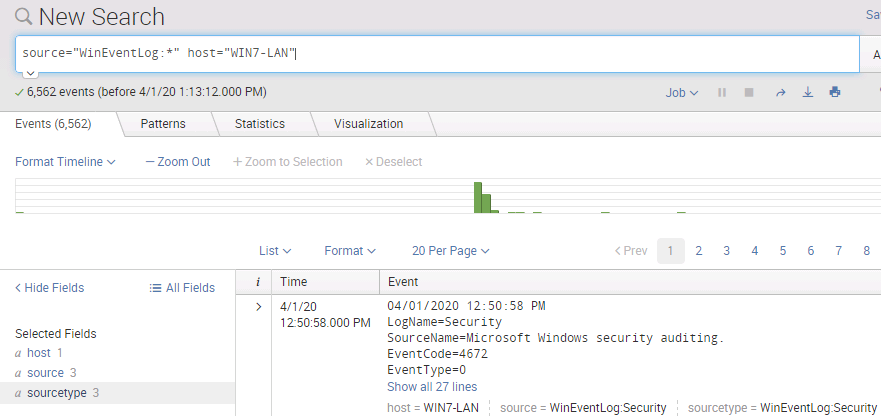


On the **Input Settings**, Selecting the following items : Application, Security, System.



No changes here

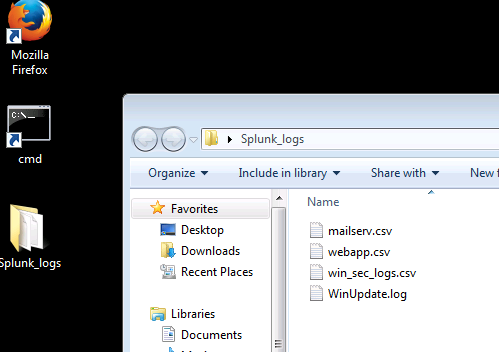




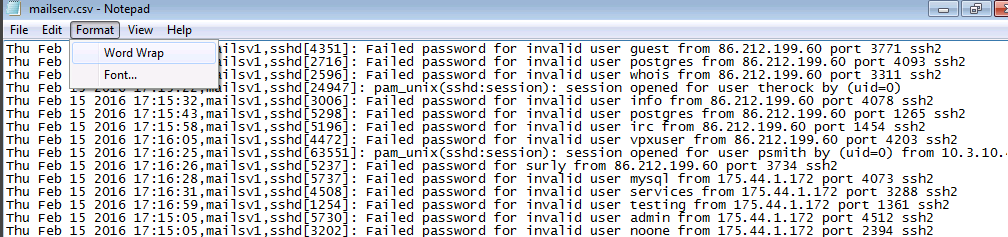
*You are exploring log file correlation and analysis using the Splunk platform to test your ability to identify indicators of compromise. You have several different types of log files to ingest into the Splunk engine for analysis. Your task is to correlate information from the various logs together in order to determine what level of unauthorized system access was obtained and what application provided the access.*

*OS: Windows 7, Splunk version 6.2.3*

I open up the Splunk-logs folder and check the data (raw form)

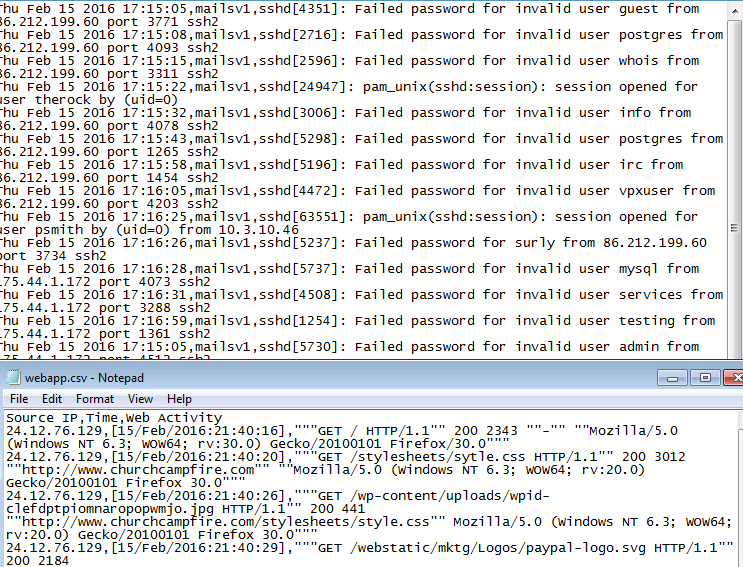


I open the “mailserv.csv” file and checked the “Word Wrap” to make all data lines visible without having to scroll sideways.



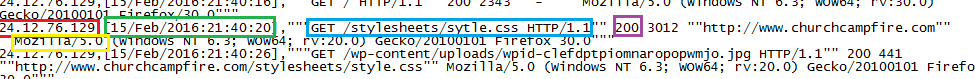
While checking the other files log, I see some suspicious entries:

* File downloads (someone is downloading the web folders to analyze it offline)
* High number of invalid login attempts (seems like an automatic password attack with a script or tool against the mail server via SSH )



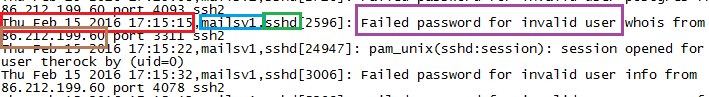
**Webapp.csv** Each line shows:

* The IP address of the webserver visited
* When the site was visited (local system time-stamped)
* GET request for item/page (with path to item/page)
* Server status code (200 == OK)
* User-agent/browser used to request item/page (Firefox, Opera)

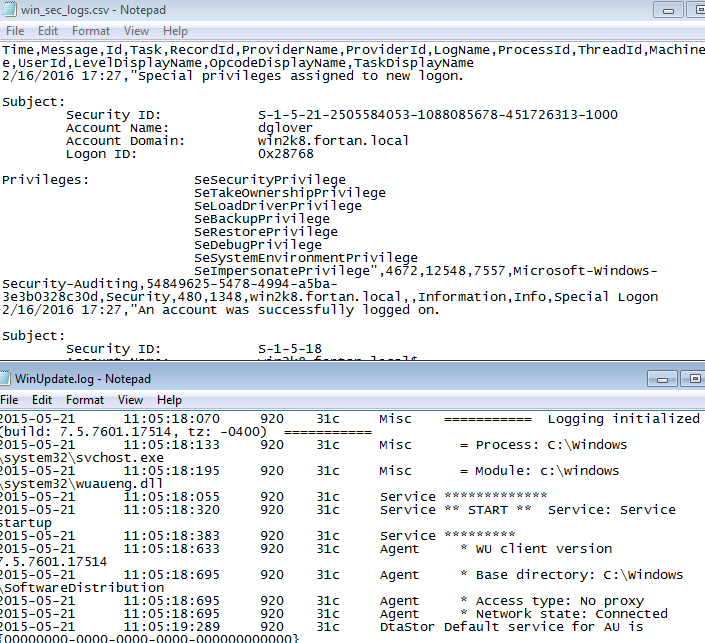


**Mailserv.csv** Each line shows:

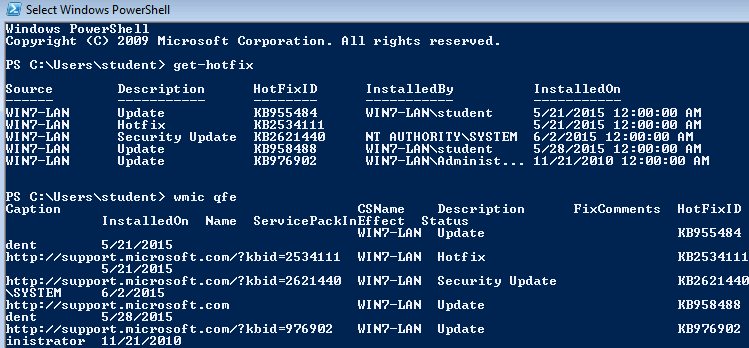
* Time/date stamp from the mail server for each item
* Server "name" (mailsv1)
* Daemon used for sending logged item in (sshd)
* Error alert verbiage (Failed…)
* IP address of the attacking machine (86.212.199.60)



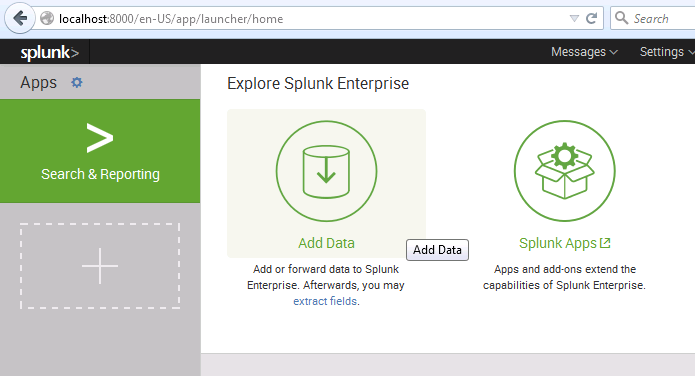
**Win\_sec\_logs** are security event log dumps from the Windows 2008 Server on the Fortan network and **WinUpdate** provides information on any missing or failed patches



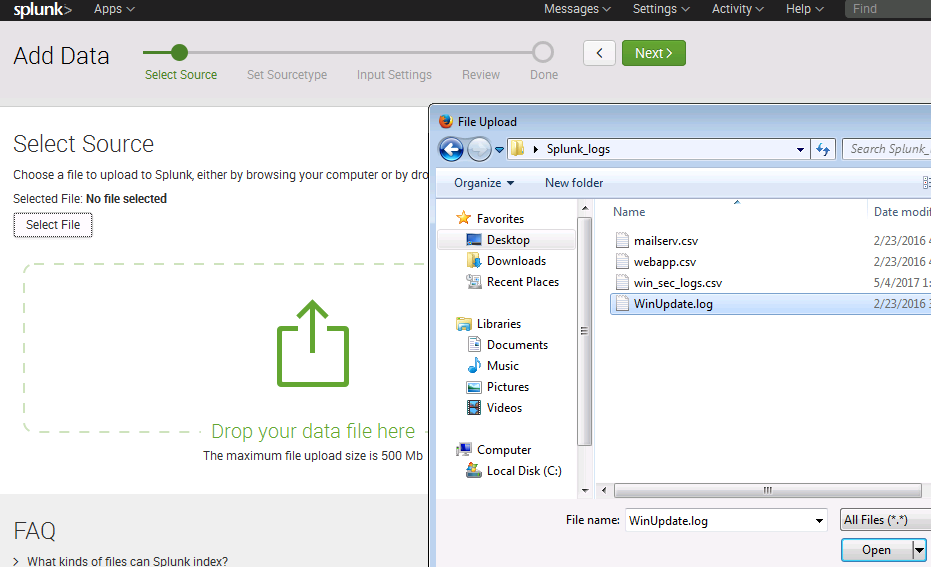
It can also get obtained with Powershell using these commands



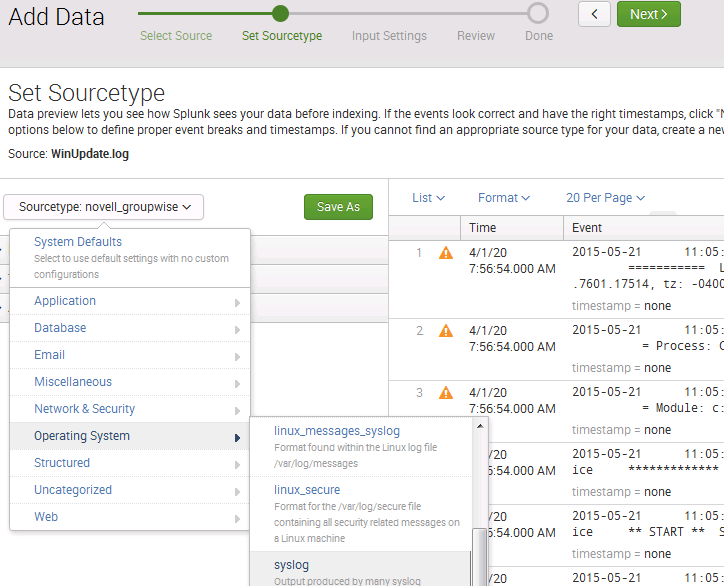
Back to the topic and Launching Splunk to add the data logs.



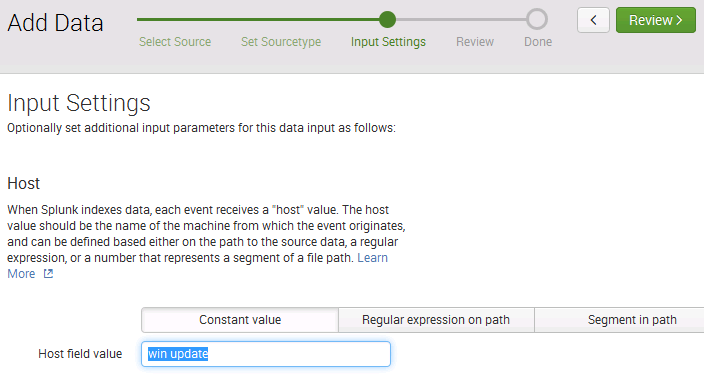
Adding WinUpdate

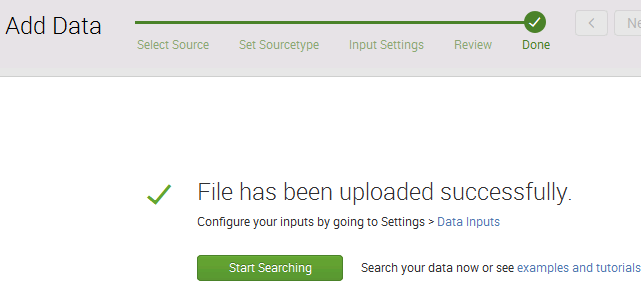


I set the **Sourcetype** to **syslog**

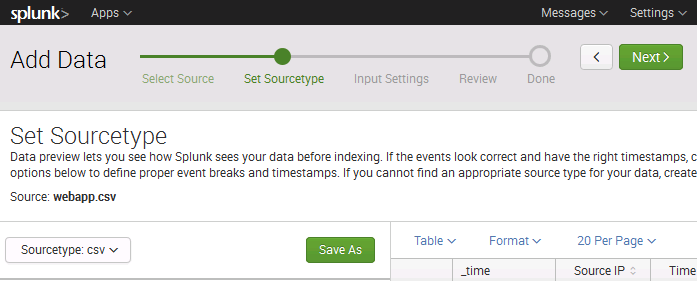


A the **Input Settings Screen**, I change the Host Field Value

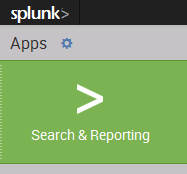




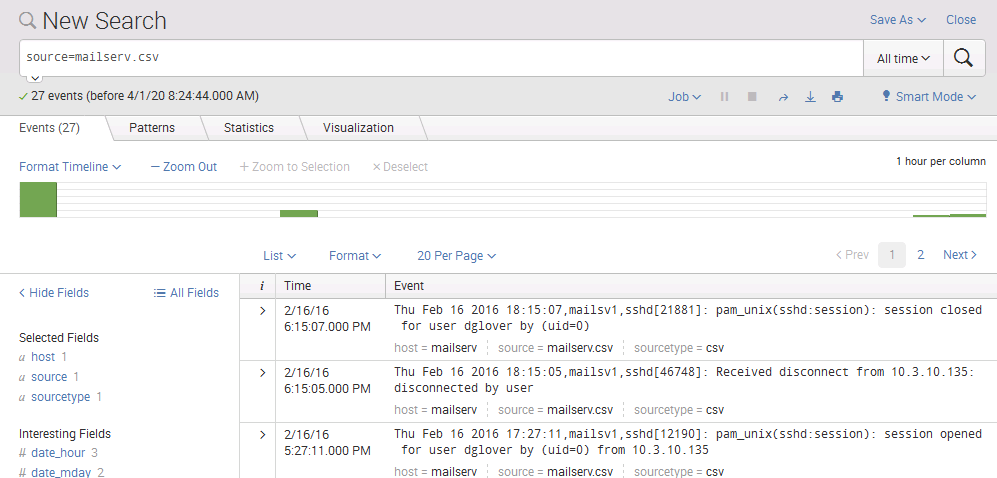
Once it is done I do the same process with **Webapp.csv** file. Unlike the previous log file, I leave it to csv Sourcetype.



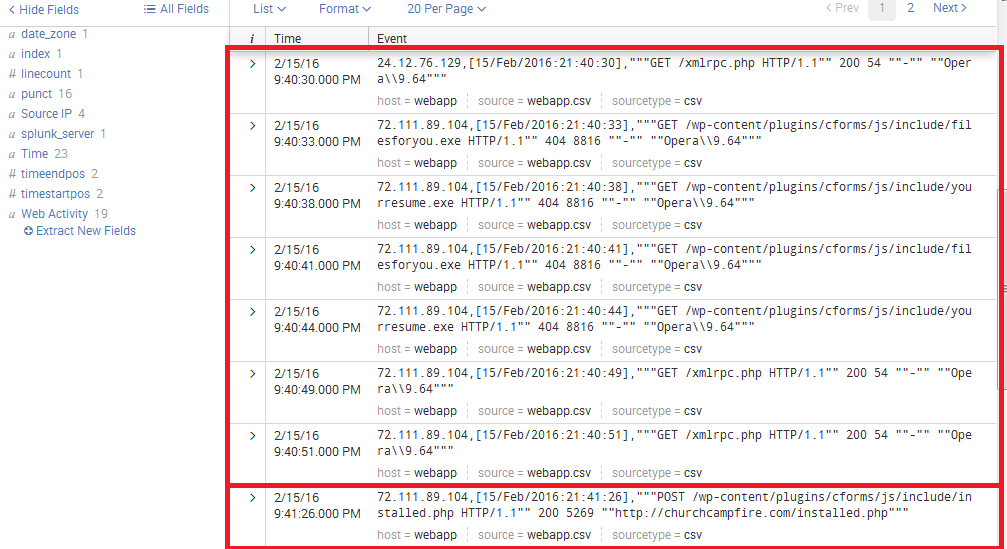
Once the four log files uploaded I click on the **Search and Reporting** tab



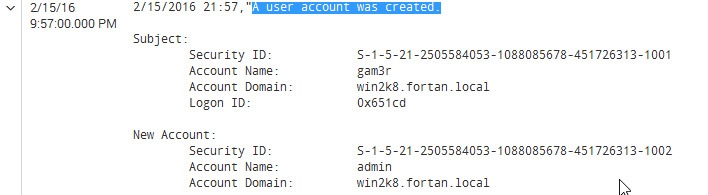
I searched for the Mailserv log file: there was a large amount of login failures in the mailserv log



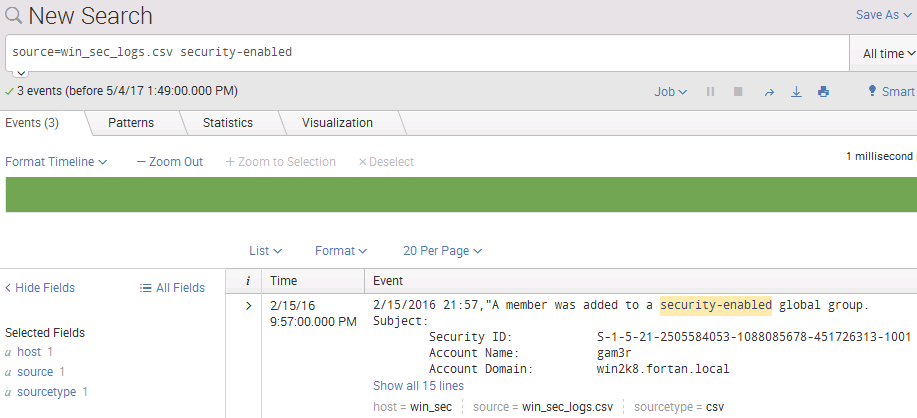
Webapp log : some suspicious files being downloaded followed by a POST activity from the Windows system to a remote page



win\_sec\_logs.csv: a user account called **gam3r** was created at 9:57 pm on 2/15/16.

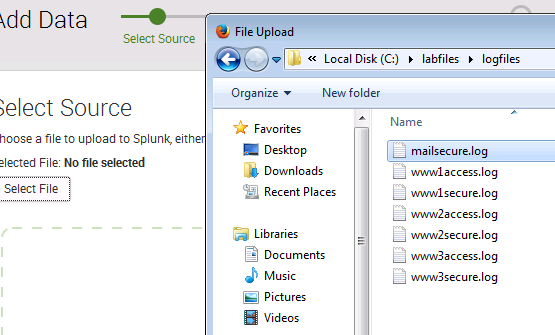


The **gam3r** account was added to the Admin group obtaining privileges.

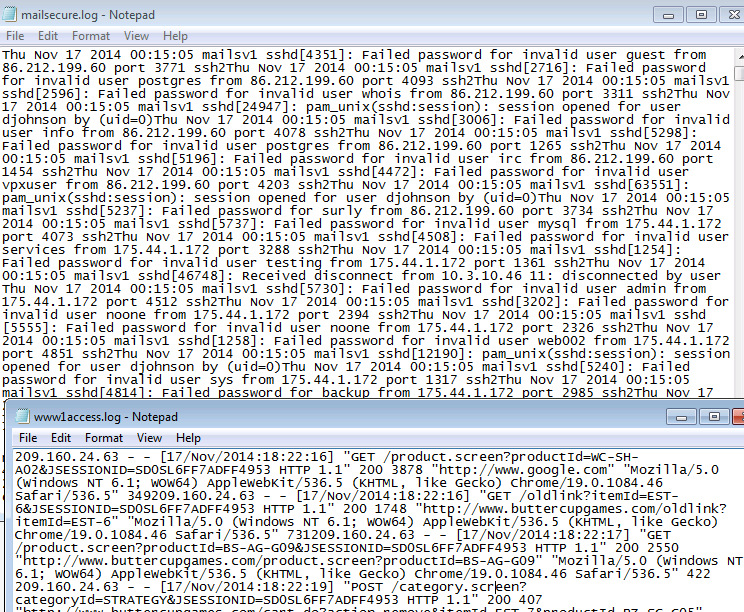


numerous attempts to gain ssh access to the mail server. We then noticed a user had clicked on a link that downloaded an application onto his computer - this happened on the same system that was reported to have suffered from erratic system behavior. Once the application was downloaded, it attempted to create a user called **gam3r** and then add it to the administrator group. After the user was added to the administrator group, the attacker would have full access to the machine. However, thanks to your sharp eye in catching the activity the application will be removed from the system and mitigations will be put into place in order to stop future breaches via this same program.

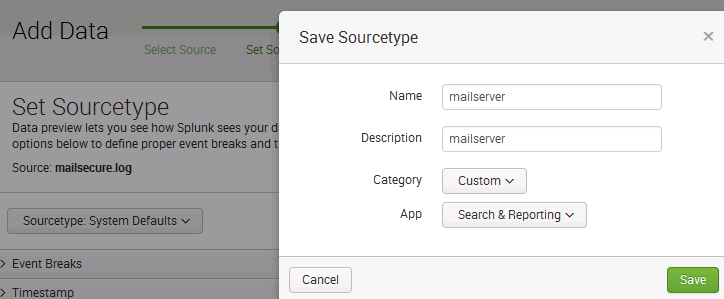
Uploading more log files



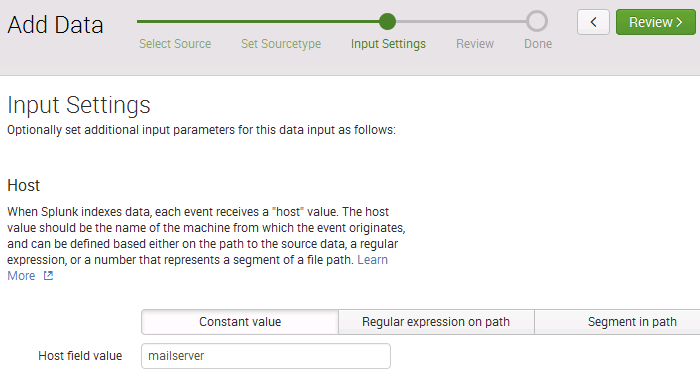
Those logs look complicated to read



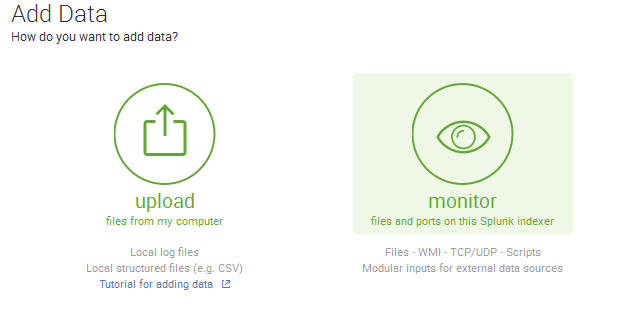
After I hit next, a dialog box appears

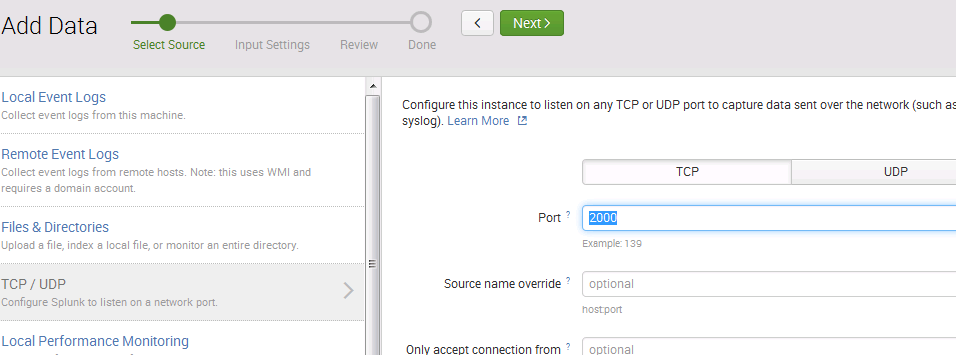


Changing the Host Field to “mailserver”

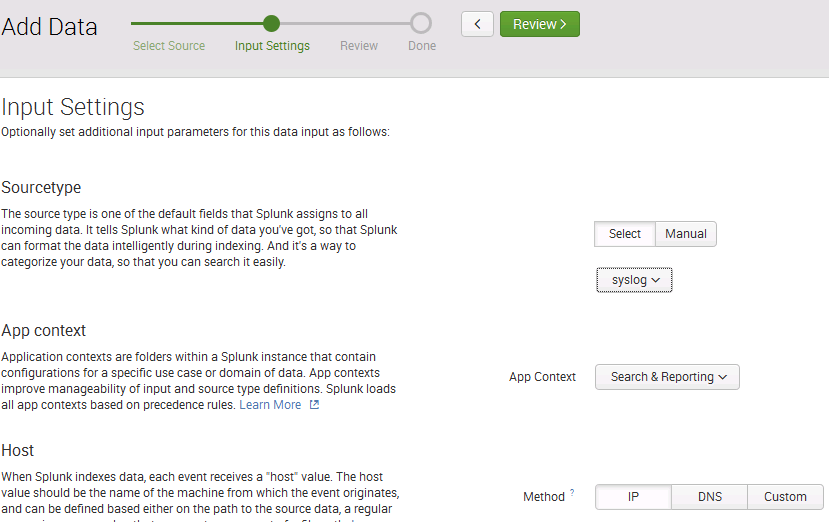


In order to get syslog data from a remote system into Splunk. I used the monitor option instead of uploading. I have to authorize TCP/UDP input. I use TCP since its is more reliable on port 20000.

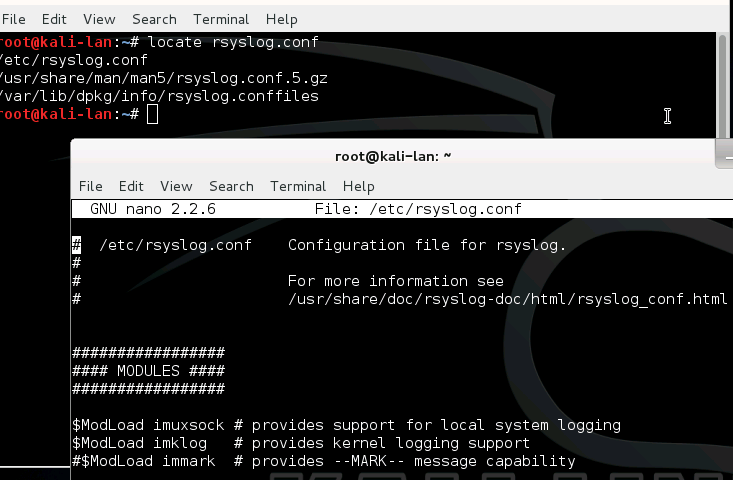




On the next page I modify the Sourcetype to “syslog” and Host to “IP”



Once it is done, I switch to a Kali linux machine and modifying the “rsyslog.conf” which logs system messages on unix systems

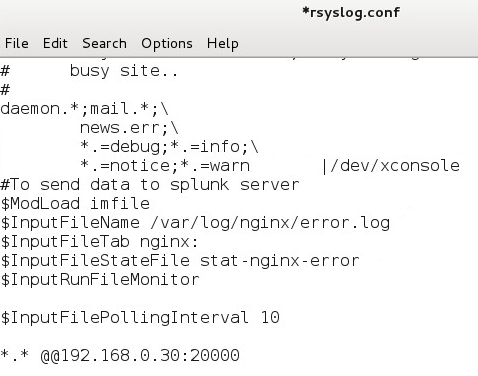


I had some issue with nano so I used another file editor and added these linse at the end of the document

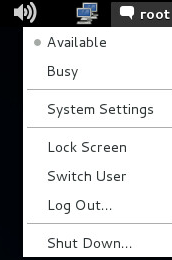
$ModLoad imfile  
$InputFileName /var/log/nginx/error.log  
$InputFileTag nginx:  
$InputFileStateFile stat-nginx-error  
$InputFileSeverity error  
$InputRunFileMonitor

$InputFilePollingInterval 10

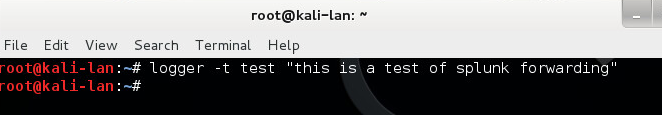
\*.\* @@192.168.0.30:20000



Right after that I rebooted the linux machine



Once it rebooted it typed the following command:



Once back in the Splunk search interface I checked if I could forward logs across a network to splunk interface. It works.

