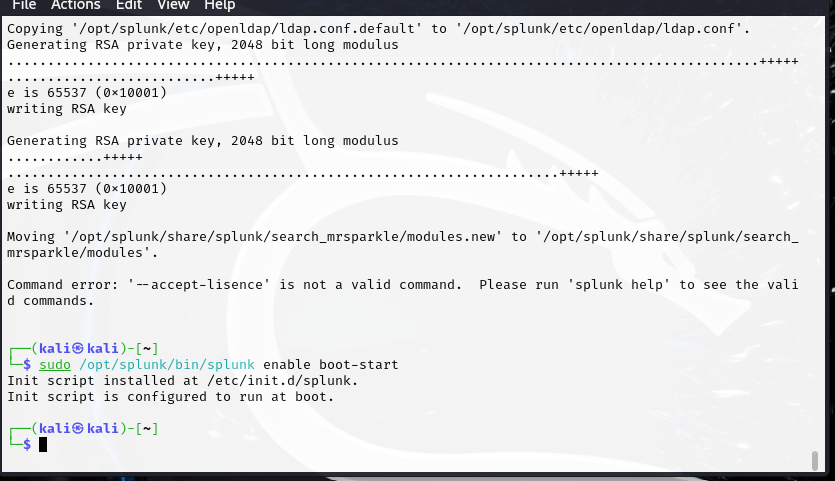
***ICS 344***

***COMPUTER INFORMATION DEPARTMENT***

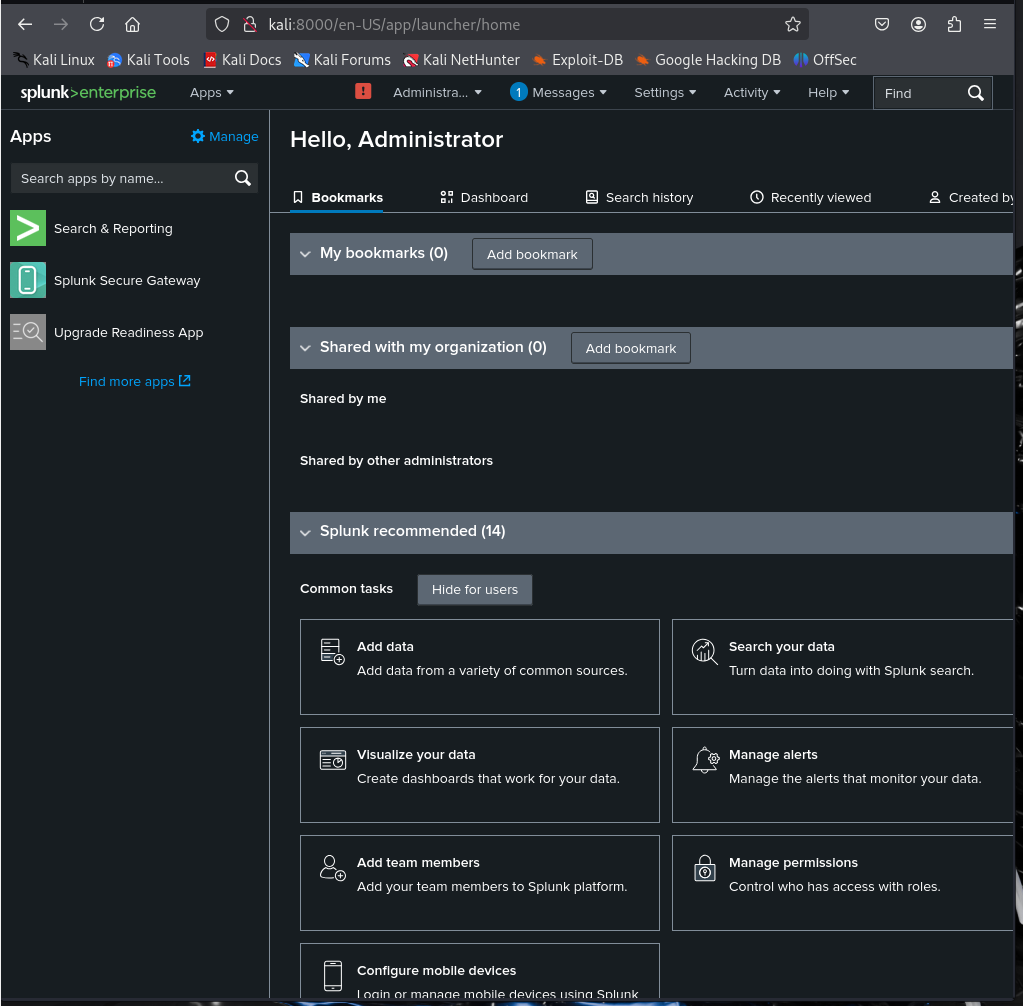
***Phase 2***

***Abdulaziz Althukair***

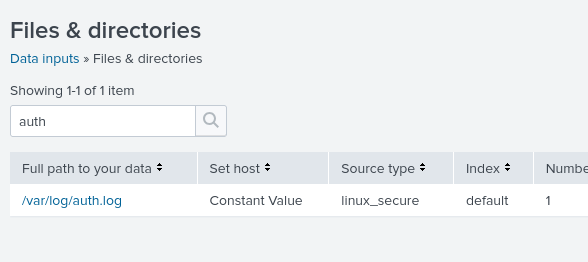
**First, we install splunk onto the victim’s PC in order to monitor traffic**



**Next, we’re able to access the web server and are able to start logging attacks**



**Then we add /var/log/auth.log to the monitored files, in order to focus mainly on brute force attacks**



**Finally, we’re now able to detect attacks from the attacker’s PC, or simply look for failed password attempts**

