410 Project Proposal

Qianyi Feng

3/8/2019

The experiments on Nagios

Introduction:

Nagios is an open source monitoring system for monitoring the computer systems and networks, and providing the alerts for the abnormal activities. It offers wide range monitoring services, such as system monitoring, protocol monitoring, application monitoring, database monitoring, log monitoring and bandwidth monitoring. From the official website of Nagios, there are more services provided in details with different demands and groups(see https://www.nagios.com/solutions/). In this project, I would focus on the installation and configuration of Nagios first, and explore other functions while Nagios could be run on my VM successfully.

I would use Nagios to monitor Linux system in this project, and the aspects would be the resources used on networks and the remote machine, and the situation of ssh. For example, if the user uses too many resources of the network services or the resources of the remote machine, then there should be some warnings that showing up on the website to remind the administrator about the abnormal activities. For the ssh part, the system should check if the VM could be ssh by other people. I would use my VM on testium as the server, and monitor the resources of my VM itself. Also, I would create several user accounts and try to make attacks to my VM, in order to test if the unusual activities made by users could be monitored successfully. After these test have been done successfully, I would try to define the functions myself. For example, the system should monitor on the specific directory. If the user attempts to write the file under this directory, then the activity would be detected, and the system should show warnings on the website, then send the email to the administrator. This function should have extended function, which is to delete the written file first, and then send the warnings to remind the administrator that the user wants to write files under this directory.

To complete the project, firstly I would make sure Nagios has been installed and configured on my VM successfully, which should be done by Saturday night(3/9). Then I would try to do the monitoring with the resources of the network and the server, the ssh function, and the due date should be next Tuesday. After that, I would use the feedback of my proposal to see if there are more things that I should focus on or something I did wrong and fix them. Then I would finish the self-defined function and extend it. If there is more available time, I would try to monitor the abnormal ssh history from users as a new function.