A Look at Implementing Security Rules and Safeguards in OpenStack for SNICScienceCloud

Aleksander Okonski
aleksander.oko@gmail.com

1 Background

Uppsala University has several high performance computer nodes (HPCs). One of the uses for these HPCs is to run the SNICScienceCloud (SNIC). This project lets researchers and professor's to run cloud based projects on the HPC recourses. The SNIC cloud uses OpenStack as its underlying cloud framework. As the SNIC project grows more users, including students, will have access and ability to spin up VMs. This poses a security problem as these users may not be aware of security rules and proper guidelines to use when initializing VMs. This has already been a small issue with several VMs beeing infected and joining bot-nets that then issued denial of service attacks on other machines. As this project grows so will the vulnerability of the SNIC cloud grow. It is therefor nectary to look into the ability to protect the SNIC cloud and ensure users are flowing best practices.

2 Proposal

OpenStack is an open source cloud computer solution that focuses on infrastructure as a service. OpenStack is used by the SNIC cloud as a platform to provide high performance computer nodes to university research and projects. This service is now expanding to the classroom where students are using SNIC cloud for cloud computing courses. As the SNIC cloud expands from research into education it provides larger security exposure. As

machines are provisioned, and deployed into this hybrid cloud they will be accessible from the Internet. This will increase the risk of machines being compromised. The proposal for this project is to assess and implement a three step solution to monitor and protect the SNIC cloud infrastructure. The first part will be to write a user guild for setting up and provisioning vms. The second part will be to implement a "watch dog" VM that would monitor the other VMs in the project. The final part would be to look into implementing a system that would allow a VM to be monitored thought the underlying hypervisor.

3 Tasks

1. Create a guide for uses to provision a VM.
2. Create the "Watch Dog" VM.
3. Ensure that the "Watch Dog" VM functions and is intuitive / easy to use.
4. Study and look into a way that the hypervisor can be used to view VM activities.

4 Time Line

1. Week 1-2 Ramp up and write documentation on different specifications that are needed in the cloud.
2. Week 3-6 Start building the "Watch Dog" server.
3. Week 7 Finish up and test the "Watch Dog" server.
4. Week 8-10 Start looking into ways of implementing a hypervisor based solution for viewing VM activities.
5. Week 10-17 Implement the hypervisor based solution for viewing VM activities.
6. Week 17-19 Fix bugs and ensure that all created components are working as expected.

7. Week 20 Finish up the report and prepare for presentation.

References

[1] https://nmap.org/

[2] https://github.com/pyKun/openstack-systemtap-toolkit

[3] https://wiki.openstack.org/wiki/Successes

[4] https://openstack-in-production.blogspot.se/2015/09/ept-huge-pages-and-benchmarking.html