# Secure Web Server and Login System

California State University Northridge

COMP 424

Professor Vahab Pournaghshband

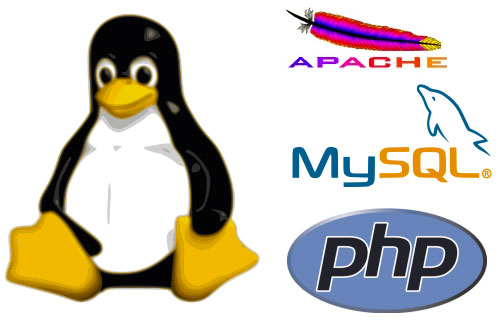
Prepared By:

Abel

Hector

Siavosh

Geneva Capos



## Snort Intrusion Detection System and OpenSSH

In current times, cyber attacks and APTs (Advanced Persistent Threats) are daily realities for any company and IT staff. Having a protection around servers and hosts has never been more important. Due to increasing efforts by hackers, simply having a firewall and anti-virus is not enough. IDSs (Intrusion Detection Systems) provide an extra layer of security. Instead of using passive means to block unwanted access, an IDS examines traffic sent to a host and determines if it is malicious or not.

Snort has been selected as the IDS for the web server. It has been selected due to it’s proficiency in detecting malicious network traffic and alerting administrators in real-time. It operates by monitoring network traffic and comparing it to saved rulesets that have been configured to describe malicious behavior. This method is far superior than relying on a firewall due to the fact that it understands what type of traffic is abnormal even if it does pass firewall rules. Hackers specially craft network packets to bypass firewall rules which often implement simple methods such as blocking all traffic to a certain port. Installing an IDS on top of other security measures is a huge step to successfully securing a system.

PulledPork accompanies the install of Snort by automatically pulling new rulesets from the Snort website. It’s crucial in a secure environment to have updated information on potential adversaries. New ways to attack systems are discovered everyday. If rulesets are not updated, the system is vulnerable. PulledPork ensures that new hacking attempts are always captured.

Splunk has also been installed to help manage alerts from Snort. Splunk is a log management and analysis software that has been praised for it’s user-friendly data visualizations. IDSs often generate large amounts of alerts, sometimes overwhelming administrators. False negatives and false positives are downsides to IDSs. False negatives are when the IDS does not flag malicious traffic. False positives are when normal traffic is flagged as malicious. It should be a priority to have a system to help administer and manage these alerts. In Splunk’s case, alerts can be monitored from a graphical interface. Alert reports can be generated in seconds and custom searches can be created to find specific patterns. This provides a huge advantage when filtering through false alerts. Splunk also used on the server to monitor critical system logs: auth.log, syslog, mysql.log and Apache error and access logs.

For remote administration OpenSSH has been installed. It’s important that web developers are always able to edit code when needed and for administrators to be able to check on system performance at any given time. SSH allows users to navigate around a host through a command line interface. Configurations of SSH services will make or break a hosts security. If default configurations are not changed, it leaves the host and potentially the whole network vulnerable to attack. The first step taken to ensure secure SSH sessions is to alter the SSH configurations. Setting up public key authentication would be the most secure implementation for an SSH server. However, to implement this one would need to know which machines would want to access it in order to copy their public key over to the server.

Works Cited

http://www.rackaid.com/blog/how-to-harden-or-secure-ssh-for-improved-security/

<http://www.cyberciti.biz/tips/ssh-public-key-based-authentication-how-to.html>

<https://www.snort.org/faq/what-is-a-snort-rule>

<https://www.snort.org/faq/what-can-i-do-with-snort>

<http://www.splunk.com/en_us/solutions/solution-areas/it-operations-management.html>