Securing LAMP:
Linux, Apache, MySQL and PHP

Track 2 Workshop

PacNOG 7

July 1, 2010

Pago Pago, American Samoa

What do we mean?

Many potential actions to secure a LAMP server. But, we will now concentrate on LAMP-specific items, including:

- Configuration changes to:
  - Apache web server
  - PHP
  - MySQL

Apache Security Items

There are a number of items we can consider, including:

- Apache access controls
- Apache mod_security module
- Using virtual hosts (already done)
- Run Apache in a chroot environment
- Using the SecFilter module
- Using ssl for https connections.

PHP Security Items

There are few configuration directives to consider. Most PHP security is in the actual code that is written. Configuration includes:

- Setting expose_php = off
- Turn off global variables
  - register_globals = off
- Be sure php logging is on.

MySQL Security Items

There are few configuration directives to consider. And, we must remember to filter user input in PHP code that accesses MySQL:

- Set a root password for MySQL
- Consider using another name for admin account than *root*.
- Remove test databases if installed.
- Make sure MySQL is only listening for local connections.

Securing LAMP Conclusion

Most or many of the items mentioned here are already done by default in the Ubuntu Linux distribution.

We will now update our configuration files to add additional security for our local LAMP installation.

Then we will create a “secure” LAMP application.