

Saturday, July 18, 2009

Testing Security with Nessus

By Solomon Chang

Nessus is a vulnerability scanner. Despite being proprietary, it is free of charge for personal use in a non-enterprise environment. Its goal is to detect potential vulnerabilities on the tested systems. It accomplishes this by maintaining its own database of every vulnerability known to its contributors (for specific mainstream Operating Systems), with each vulnerability rendered into executable scripts. After selecting the vulnerabilities you want to test for, you simply launch... and wait. Nessus then returns a report of any backdoors, admin passwords, etc. that it has found, as well as helpful links to instructions on how to patch them.

Nessus is meant to be a security-testing tool that you deploy against your own machines before you put them on the public internet. It is not meant to probe other people's machines, although this is very commonly the case. Solomon will briefly discuss other security tools and common probing techniques, as well as protecting yourself against probes.

When he is not teaching Defense Against the Dark Arts 101 at Hogwarts, Solomon Chang is a MySQL certified DBA and the current acting director of LAMP SIG. He works as a professional Database Administrator four stories underground in an organization he is not allowed to talk about, and is a co-author of the MySQL Cluster Certification Study Guide.

Posted by Solomon K. Chang at 13:00