COMPUTER SECURITY AND HONEYPOTS

Arun Darlie Koshy [1,2]

[1] Team ISW, Infosecwriters.com
[2] Department of Mathematics and Statistics, RMIT University

EXTENDED TUTORIAL ABSTRACT

A Honeypot is a security resource whose function is defined by it's unauthorized use. The concept is considered by many to be at the cutting edge of network security research.

In comparison to existing techniques in network security, Honeypots differ as they do not produce false alarms. This is because any kind of activity directed towards them is by definition malicious.

We look at their taxonomy : namely "production" and "research" honeypots. A special emphasis is given to the concept of honeynets. They can be simply thought of as decoy networks formed out of honeypot components (routers, nodes et.al).

Certain key requirements of a honeynet are data control, capture and collection. These are the attributes that allow the maintainer(s) of the honeynet to study attacks (and attackers) as they occur and in contexts not possible before.

This tutorial hopes to introduce the audience to the topic by giving a broad overview of the subject. It will also feature specific research from the Honeynet alliance and ISW's Honeynets @ home project.

A kit containing relevant papers, tools and demos will be made available to interested members of the audience.