Pubcast Secfault - IDS Overview

Monday, 09 November 2009

Pubcast: Secfault, the Durban leg of the Pubcast has been created to address the more technical aspects of security which the Pubcast has tended to overlook.

In Episode 2 Matt and Ralfe discuss IDS, a critical component of any security armament. The team considers the function of IDS, it's placement in the network, deperimeterization, impacts to the infrastructure and the future of this technology

As our lives become ever more frenetic, our demands for computing portability increase. Similarly, as our demands for integration increase, data portability follows suite. These movements away from traditional architectures towards a distributed configuration leads to deperimeterization, ultimately moving the responsibility of security from specialized security devices typically found on the perimeter to the software systems themselves. In this episode we take a look at Intrusion Detection Systems, how they have been traditionally used and where they are heading.

Contents

- What is IDS, and what types of IDS do you get?
- Intrusion Detection Systems detection methods: Anomaly vs. Signature.
- Matt describes some experimentation he’s been doing with the placement of the snort detection sensor.
- Introducing Deperimeterization and it’s increasing influence on the use of IDS’s.
- The distribution of data and devices leads to a change in infrastructure, causing security to move from the perimeter and into the software systems.
- The responsibility of security is moving away from security devices, and is now becoming globally integrated.
- Limitations of IDS. It is not the silver bullet, but is one of the weapons in our artillery.
- We end off with a quick explanation of the difference between an Intrusion Detection and Intrusion Prevention System.

Links

Deperimeterization : http://www.opengroup.org/jericho/deperim.htm

PHP-IDS : http://www.php-ids.org/

Pubcast Episode 21 (Full)

Download the Full Audio File

{audio}http://www.discussit.co.za/_media/_audio/itsp/Pubcast_Episode_21.mp3{/audio}

Pubcast Episode 21 (Part 1)

{audio}http://www.discussit.co.za/_media/_audio/itsp/Pubcast_Episode_21_1.mp3{/audio}

Pubcast Episode 21 (Part 2)

{audio}http://www.discussit.co.za/_media/_audio/itsp/Pubcast_Episode_21_2.mp3{/audio}