PacNOG-20

TRACK 2 - NETWORK SECURITY WORKSHOP

Synopsis:

The objective of this workshop is to examine the key concepts, protocols and the policies involved in establishing and maintaining security for a network, and building an understanding and familiarity with their operation. Device and network infrastructure security is examined with a focus on different layers to establish a robust, stable and secure network and protect the data and processes that occur in the network.

The workshop also looks at the nature and structure of network attacks and the motivation that drives such on-line malicious activity.

The course further examines the actions and processes that can be used to identify, mitigate and respond to such attacks.

Target Audience:

Engineers, Network Managers and Operators, Security policy makers who are interested in network security and gaining an understanding of the threats they face and how to mitigate such threats.

Pre-requisites:

It is assumed that participants have a basic understanding of network operations and Internet technologies.

Course Outline:

- Threat Models
  - Types of Attackers
  - Network Infrastructure
  - Service Infrastructure (e.g. DNS, email)
  - Users
- Network Infrastructure
  - Router and Switch Protection

    - Routing Protocol Protection
    - Detecting Sick Hosts and Walling Them
- Infrastructure Services
    - IDS
    - Firewalls
    - IPv6 Security
    - Anomaly Detection
    - RPKI
- End User Hosts
    - Mac, Unix, and Linux
    - Keeping Up to Date – Patching
    - Host Based Firewalls
    - Authentication Services
    - PKI Services
    - Checking for Disease: Scanners
    - Preventing Disease: Anti-virus
    - Safe Mail Practices
    - Safe Browsing Practices in Firefox, Chrome, Safari
    - Safe Inter-host Protocols: SSH, RSVC, SFTP and more
    - Personal Encryption of Files and Communications
- Administrative
    - Security Plan
    - Inter-network Cooperation
        - NOGS
        - CERT
        - FIRST
- Security Personnel
- Planning for Future Changes

Other requirements

Hardware: It is highly recommended that participants bring their own laptop computers with Wifi (b/g/n) and administrative access to system to practice the lessons learned during the workshops.

Software: SSH Client, Telnet Client

Maximum number of attendees:

36 delegates per workshop