TRACK 3

Agenda
2. Incident Management and Response: 01-02Dec 2016

1: Network Security workshop

Venue: PacNOG 19 Tanoa International Hotel, Nadi FIJI
Duration: 2 days; Track #: 3 [29-30Nov 2016]

Trainer
Mr Fakrul Alam; Training Officer, APNIC

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:
- Network Security Fundamentals
- Security on Different Layers and Attack Mitigation
- Cryptography and PKI
- Device and Infrastructure Security
- Operational Security and Policies
- Virtual Private Networks and IPSec
- Network Security Incidence handling and response procedure
2: Incident Management and Response

Venue: PacNOG 19 Tanoa International Hotel, Nadi FIJI
Duration: 2 days; Track #: 3 [01-02Dec 2016]

Trainer
Adli Wahid, Security Specialist APNIC/FIRST

This training is a FIRST.Org Training Module

Prerequisites: It is assumed that participants have a role in setting up and managing operations in internet security in their organisations and would have existing technical understanding of internet networks, operations and systems.

Module 1: CSIRT Fundamentals

This module examines what incident management is and how it fits into various frameworks, defines what a CSIRT is and its role in incident management, and steps through organizational planning issues around creation of a CSIRT.

Module 2: Starting with a CSIRT

This module walks through how CSIRT leaders and managers would set up and manage a newly created CSIRT. It covers both the external processes of meeting the needs of stakeholders and community and the internal processes of policies, configuration, and planning.

Module 3: CSIRT Operation

This module steps through the incident management process in detail, including how to improve incident handling techniques, and also steps through best practices for publishing communications about incidents, working with the media, and testing and verifying incident management processes.

Module 4: Working with Information Sources

This module steps through how to work with information sources to gather critical information, including open-source intelligence and proprietary intelligence. It also examines processes for information exchange.

Module 5: Incident Coordination

This module focuses on how to handle major security events and coordinate incident responses with external entities such as vendors, law enforcement, and various types of organizations.

Module 6: CSIRT Performance Measurement

This module establishes methods to measure and improve the effectiveness of a CSIRT by using performance analysis and maturity models.