



APNIC Brisbane, Australia 11-13 August 2008

APNIC Training
in conjunction with
APTLD



Technical Security Workshop for cctld operators

Venue: APNIC Offices, Milton, Brisbane, Australia

The objective of this workshop will be to provide cctld operators and other interested participants with the understanding and operational skills needed to plan and implement the processes and procedures required to maintain a secure, robust and available production environment. The workshop will be practically orientated with hands on exercises using the APNIC training lab.

Main topics to be covered will be:

Device security –

Establishing robust, stable and secure network devices and protecting the data and processes that occur on these machines.

Network infrastructure security –

protecting a network against intrusion and controlling the flow of traffic in a network and across network devices.

Network forensics –

understanding the nature of the activity on a network, analysing network traffic and identifying anomalies and attack patterns.

Attack mitigation –

establishing responses and actions that can be rapidly deployed in the event of an identified attack. This can also include steps to ensure rapid recovery and continuance of service.

Exercises will cover

Device security configuration, botnet operation, preventative measures, flow collection, use of nfdump and nfsen, DDoS source identification, sniffing,
Further topics specifically relevant to cctld operation will also be included.

Online registration (open mid July) and more information

<http://www.apnic.net/training> or email training@apnic.net