Training for CSIRT staff

Andrew Cormack, Jacques Schuurman, Claudia Natanson, Wilfried Woeber
TF-CSIRT
CSIRT staff are different

Not just sysadmins
Not just network techies
Though we take both of those for granted
  ■ Or learn them elsewhere
Filling in the gaps is important
Target Audience

Members of new teams
New members of existing teams
Assumed already to know how the Internet works
  - Course teaches how it breaks
Based in Europe
  - CERT-CC series of 3&4 day courses in USA
Course Objectives

Students should learn

- Tasks involved in operating a CSIRT
- Skills needed by CSIRT staff
- Tools and techniques of incident response
- Need for links with other organisations
Course Modules

Legal Issues
Organisational Issues
Technical Issues
Market Issues
Operational Issues
Legal Issues

Rules & laws
Harmonisation
Jurisdiction
Powers of investigation
Contacts with law enforcement
Access to and use of restricted tools
Organisational Issues

Your ISP
Your constituency
Assets and risks
Risk management
Security policy templates
  ■ For your customers
  ■ For your team

RFC2350
Public functions
Press contacts
Sister organisations
FIRST etc.
Staffing issues
Technical Issues

Operating Systems
- About the OS
- Network stacks
- Vulnerabilities & back doors
- Integrity

Forensics & Data mining

Networks
- IP/ICMP
- TCP/UDP
- Higher level protocols
- Masquerading & hijacking

Encryption

Certificates & PKI
Market Issues

Vendors
Commercial teams
Security bulletins
Undisclosed vulnerabilities
Other sources of information
Operational Issues

An operational framework

Incident response
- Reporting templates
- Tracking & Bookkeeping
- Taxonomy

Management reports

Other activities

Trust brokers
Finding contacts
Other (reliable) sources of information
Course format

Modular to ease delivery and maintenance

Modules include

- Presentations
- Workshops
- Discussion

Full course takes two days

- Allows informal discussion in evening
Progress and plans

Initial development by TF-CSIRT sub-group
Draft syllabus for discussion in January 2001
Development of modules by community
■ Perhaps professional advice for legal section!
Aim for delivery during 2001