FIRST Member Future Services

Forensics for IRTs

Workshops

Background

- FIRST Conference 1998 AGM
- Funding model
- Fees and conference profits
- Voluntary effort
- New services for membership

Forensics Workshop

- Intended audience
- Location & Timing
- One off vs. repeated
- Global membership

Intended audience

- Public or FIRST only?
- Experienced members or new recruits?
- Presentation or participation

Location

- Add to TC - already “closed”
- TC host willingness (or even permitted)
- Conference - before or after?

One off or Repeated

- One off is a big effort for the organisers and leaders
- Re-useable material and presentations more work for the originators unless lee-way for content
- Relevance to current incidents

First Approximation (!)

- October TC
- Intent to give FIRST members framework to share expertise and ideas - Hands On!
- Costs to cover local and organisational expenses
- 3 teams/perspectives - victim, attacker and IRT - simultaneous or sequential (time?)

Hardware & tools

- Should not be too platform / OS dependent - generic approach
- Simulated victim - all too easy - lots of hidden extras!
- Attacker - much harder to simulate
- IRT - good ones and poor ones ;-)

Workshop Team

- Co-ordinator
- Duplication / overlap for each category
- Voluntary effort may be re-prioritised
- Pre-workshop time to create hosts, network flows, mini-Internet (DNS, NIC, etc)

Intellectual Property

- Need a clear statement of I.P.
- FIRST.Org Inc. ?
- Needs to be available to all teams in some way - quasi-franchise?
- Sanitised data

Comments & feedback??

- Over-ambitious?
- Feasible?
- Desirable?
- Volunteers?
- Sponsors?
- Other?

Working group

- First-nswg@first.org