ISP Security BOF – NANOG 28

- Time: Monday 7:30 - 9:00
- Place: Granary Conference Room
- Facilitators:
  - Merike Kaeo kaeo@merike.com
  - Barry Raveendran Greene bgreene@senki.org
- Objective: Meet, Consult, and Endeavor to work more efficiently to keep our Net alive.

ISP Security BOF – NANOG 28

- Introduction
- NSP-SEC Review – Rob Thomas
- NIAC Vulnerability Disclosure Framework – Jim Duncan
- Questions from Peers to Peers
- AOB

A year ago ….

- It was hard for ISP Security engineers to find their peers.
- DOS/DDOS mitigation was mostly done in one provider’s network.
- Lots of networks were still using ACLs as their only security mitigation tool.

Today …..

- ISP Security engineers can find each other via NSP-SEC.
- Inter-provider mitigation is a norm (i.e. several providers work together to lock down an attack).
- Active measure are in trial to automatically black hole Botnet creation
- ISPs have a *bag of security mitigation tricks*.
- Then again, *Gigbots* are not surprising.

Life is not perfect ….

- We’re here to find small increments to make life easier.
- We’re not here to solve the Internet’s security problems. Way to big a problem.
- The ISP Security BOF looks for the *small things* that will add up over time.

NSP-SEC

- NSP-SEC – Closed Security Operations Alias for engineers actively working with NSPs/ISPs to mitigate security incidents.
- Multiple Layers of sanity checking the applicability and trust levels of individuals.
- Not meant to be perfect – just better than what we had before.
- http://puck.nether.net/mailman/listinfo/nsp-security

NSP-SEC-DISCUSS

- Operators and related colleagues working on the next:
  - New technique
  - Inter-Provider procedures
  - Operational practices
  - Potential BCPs
- http://puck.nether.net/mailman/listinfo/nsp-security-discuss

iNOC DBA Hotline

- ISPs needed to talk to each other in the middle of the attack.
- The iNOC Hotline was used to get directly to their peers.
- Numbering system based on the Internet:
  - ASnumber:phone
  - 109:100 is Barry's house.
- SIP Based VoIP system, managed by www.pch.net, and sponsored by Cisco.
- Donate a Cisco 7960 to your customers and plug them into the global ISP NOC hotline.