APAN security activities: APAN NOC report

Yasuichi Kitamura (kita@jp.apan.net)
APAN Tokyo XP
Tokyo XP centric L3 connections

- USA
- Japan
- Australia
- Korea
- China
- Europe
- Russia
- Taiwan
- Thailand
- Singapore
- Philippines
- Malaysia
- Nepal
- Internet:-)
Operational security issues

• Spam Mails
• DoS
• illegal access
• illegal navigation
Spam mails

• The mailing list address of the operator group is opened.
• Spam mails occupied the mail traffic.
• Spam mails sometimes carries the virus, too.
✓ Spam filters and anti-virus softwares were set against this.
But...
Spam mails

- Especially, in APAN area, in some cases, researchers or engineers are using hotmail and yahoo. netscape.net, too.

- If they are showing their real names with their characters, the spam filters marked those mails as the spams.

- No mails to the operators were discarded without being checked.

- Someone is always seeing...not reading.
DoS

• DoS itself is critical for network services but, in the fat pipe network, it is sometimes very hard to detect this attack.

• DoS attack frequently happens especially against IRC servers.
  • Shutting down the announce of the prefix of the servers is the solution.

• Trial of accounting flow
  • [http://vabo1.jp.apan.net/flow/](http://vabo1.jp.apan.net/flow/)
illegal access

• Illegal access trial happens against routers, servers.

• Operators are required to use ssh for accessing those machines.

• All ports except service ports are closed.

• Access control for those machines are managed with using “host.allow” file.
illegal navigation

- illegal routing table injection
- wrong configuration, experiments?
- illegal name database injection
Items against operational security issues

- ssh
- filter against the illegal AS paths
- packet filtering for the management segments
- BGP MD5 peering
- Multicast
  - rejects of the bootstrap for the RP
  - detection of the bogus MSDP SA
- quick version up of the router OS and the server OS
options

- access control against the NOC building or floor
- biometric information registration
- tracking the engineer activities for one month.
Requirements of the collaboration

- smart spam mail filters
- flow monitoring between NOCs
- DoS detection in the fat pipe:
- DNS monitoring