Security management in DMZ network

- Especially in public servers (DMZ servers), server admins have to spend a lot of effort to maintain the security.
- It may be efficient for the security to be managed in command-hierarchical manner, however, it may reduce variety and flexibility.
- In some of research institute, like KEK, DMZ servers are operated like below:

  - Various usage: experiment, login shells, public relations, etc.
  - Various kind of research: various users
  - Various kind of groups: e.g. num of members are 10 - 1000
  - Login shell with binding of accounts in various countries
  - Various level of management skill

DMZ User’s Portal

to maintain security with keeping variety and flexibility of DMZ hosts

- We need to operate and a vulnerability scanner for DMZ server admins.
- Because of rich functions themselves, the vulnerability scanner is intricate to use.
- To simplify, we develop DMZ User’s Portal that wraps the functions and promotes self security management for DMZ admins, as the points below:

  POINT1: provide easy-operation user-interface to manage and handle the vulnerabilities by DMZ admins themselves

  POINT2: with harmony of support and command-hierarchy
  - Support: DMZ admins can conduct vulnerability scan by their own.
  - Support: The Portal collects and aggregates the info to maintain the security.
  - Command-hierarchy: the Portal helps the duty for DMZ admins to self-inspect their hosts annually, by providing the management interface.

  POINT3: feedback the vulnerabilities of their host in multi and continuous way
  - Three scanners are set in WAN, DMZ, LAN, which assume attacks from the locations.
  - Regular scan per week by the Portal / on demand scan by admin.
  - The vulnerability list can be browsed together / downloaded in each host.
  - When serious vulnerabilities are found on a DMZ host, the Portal notifies the info per week by email.

- Various feedback ways shown above help to determine the priority to measure.

System design of DMZ User’s Portal

- Using self inspection: the Portal helps the duty for DMZ admins to self-inspect their hosts annually, by providing the management interface.

  - Command-hierarchy: the portal helps the duty for DMZ admins to self-inspect their hosts annually, by providing the management interface.

Class structure of DBPowder (O/R mapping)

- Except for base classes, code generator generates all of codes.
- Entities can have a relationship between them.

Self inspection

~ a story of admin task in one year (April to March)

- Got into a serious vulnerability: MTM server was not corresponded

  XXth, May

  - Anonymous of self inspection
  - Apply security updates and run an on-demand scan
  - A vulnerability with 500 pt was left
  - Conduct a config and conducted treatments
  - Ran on-demand scan again and the score reduced to 10 pt

  22th, Nov

  - Treated with small vulnerabilities
  - Ran on-demand scan again
  - The score reduced to 1 pt
  - Noted that remained vulnerabilities would not cause serious problems
  - Then, submitted the report

  December

  WWth, Feb

Statistics of the self inspection: submit a report

- Started in 2005 (fiscal year)
- Security managers in divisions help the operation a lot
- Num of hosts increases every year
- Most of hosts end in 1 or 2): submission is completed

  1) under 1000 pt
  2) with vulnerabilities with red score left
  3) supplemental report
  4) a report that explains false-positives

Conclusions

- In research institutes, variety and flexibility are crucially important — also in DMZ network
- We developed and operated DMZ User’s Portal
- With harmony of support and command-hierarchy
- Feedback the vulnerability information of their host in multiple and continuous way
- Operation over 10 years shows the validity
- Flexible implementation enables to expand DMZ User’s Portal to other sites