The design and development of Vulnerability management system

Thursday, 4 April 2019 14:00 (30 minutes)

There are always many vulnerabilities in the operation system, applications and network devices, and vulnerabilities are great threats for security. The vulnerability management and lifecycle tracking is very important and necessary for the security team.

The paper describes the design and development of the vulnerability management system. The functional modules of the system includes information system asserts management, vulnerability detection, vulnerability handling and tracking, vulnerability statistics and visualization. Asserts management modules as a basic part of this system, discovers and stores the existing IT asserts (Hardware information, Operation information, IP address, TCP port services, URLs and so on). Vulnerability detection module discovers the vulnerabilities in the IT asserts using some open-source and commercial tools. The vulnerability handling and tracking module distributes and tracks the vulnerability until all the vulnerability tickets are closed. The statistics and visualization module serves for the security team, which provides data analysis results diagrammatically to show the proportion of each vulnerability category and the vulnerabilities trend during a period of time.

Partial functions of the system have been developed and deployed in IHEP information environment.

Summary

The paper describes the design and development of the vulnerability management system. The functional modules of the system includes information system asserts management, vulnerability detection, vulnerability handling and tracking, vulnerability statistics and visualization. Asserts management modules as a basic part of this system, discovers and stores the existing IT asserts (Hardware information, Operation information, IP address, TCP port services, URLs and so on). Vulnerability detection module discovers the vulnerabilities in the IT asserts using some open-source and commercial tools. The vulnerability handling and tracking module distributes and tracks the vulnerability until all the vulnerability tickets are closed. The statistics and visualization module serves for the security team, which provides data analysis results diagrammatically to show the proportion of each vulnerability category and the vulnerabilities trend during a period of time.

Primary author: Ms HU, Hao (Institute of High Energy Physics)

Co-authors: Mr ZHAO, Chengcai (IHEP); Ms CHENG, Manman (IHEP); Dr YAN, Tian (IHEP)

Presenter: Ms HU, Hao (Institute of High Energy Physics)

Session Classification: Networking, Security, Infrastructure & Operations

Track Classification: Network, Security, Infrastructure & Operations