Minutes:9/12/2010

Writer: Hoang Ngoc Kim

Content:

* Alert Rule data flow:
  + The format of IP Range is like 192.168.1\_10
  + Source Port and Dest Port is just one port
* Packet data flow:
  + Change the format according to IPv4, IPv6 packet structure.
* Modify Vulnerability Info base on OSVDB.
* Vulnerability Info is used to define the severity of the attack (Thi).
* The format of Server Info is the object\_correlation in OSVDB.
* Server Data: base on the File System Monitoring in paper HIDS collection method.

Task:

* Everyone researchs about HIDS.

Add new rules:

* The day when Kim writes the minutes, he must ask someone in group to bring the laptop.
* The person who write the minutes must write his name in that minutes.
* The order of writing minutes: Thi-Kim-Tan-Q.Thang-C.Thang.