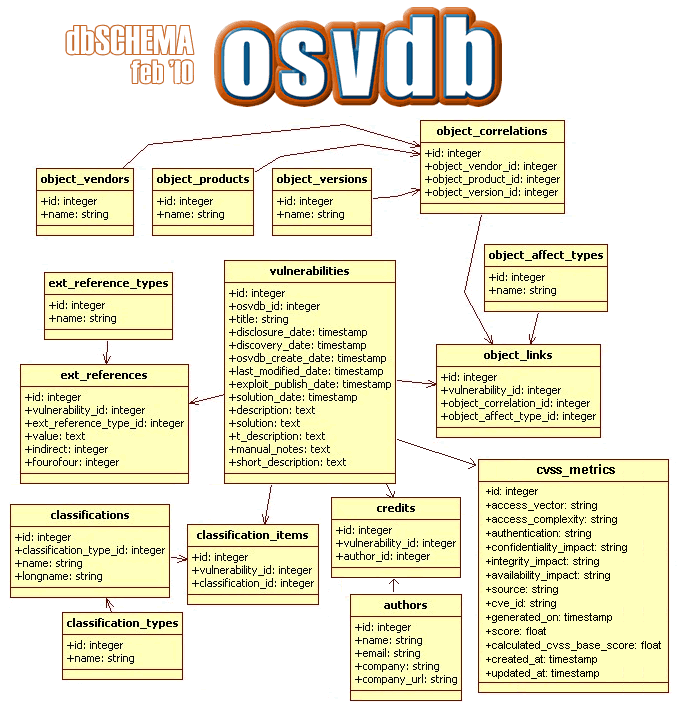
**Vulnerability Info**

Dòng 1:

Từ Process 5-> D2

Đề xuất dòng dữ liệu này sẽ bao hàm toàn bộ dữ liệu lấy về từ cơ sở dữ liệu trên mạng(OSVDB chẳng hạn),và có cấu trúc tương tự như cấu trúc lưu trữ của các cơ sở dữ liệu trên .

Vì trên thực tế chúng ta lấy phần lớn dữ liệu về vuls tại nguồn này .



Dòng 2 :

Từ D2->Process 6

Dòng này đề xuất sẽ chỉ trích một phần dữ liệu liên quan đến vuls gồm đề cử phần “object\_links” ,cụ thể chỉ để có thể suy luận với soft đó , version đó thì có vuls gì.

Nếu có thêm yêu cầu cụ thể truy suất thong tin thì mới lấy phần thong tin còn lại .

Thêm một vấn đề có lẽ đã được đề cập Vul của server không chỉ để visualize mà còn dùng trong Make Graph <đây là trên lý thuyết>

**Server Info:**

Nếu theo phương án trên thì phần Server Info này sẽ bao hàm các thong tin liên quan có cấu trúc giống thành phần “object link” như trên để process 6 tiến hành match đưa ra các vul hợp lý

Nếu cầu có thể thêm phần thời gian quét để tiện log hoặc kiểm tra sự thay đổi version tương ứng theo thời gian chẳng hạn

**Server Data:**

Theo như tìm đọc về các HIDS thì nó sẽ tạo các bản snapshot của các file cấu hình hệ thống ,log account.… .Sau thời gian sẽ quét lại so trùng xem có sự thay đổi nào không => đưa ra cảnh báo .

Vì thế thong tin có thể là các file hệ thống trên hoặc các bản hash của các file đó.

=>Chưa xác định rõ cấu trúc hợp lý

“A Host IDS is a security monitoring program that scans important operating system files, storing a signature (checksum or hash) of each file.

Every few hours, the scan is repeated. Any changes to the files will result in a different signature. The user or administrator is alerted about the changed files (notification via email is possible). Newly created and deleted files are also reported.

It is the administrator's responsibility to analyze the changes and to determine whether or not the changes are harmful.”