* Cài đặt Snort trên Unix:
  + Tùy vào phiên bản Unix hiện tại của máy có thể sẽ phải cài thêm một số thư viện con cần thiết , trong quá trình cài đặt (configure /make/make install) nếu thấy thiếu thằng nào thì sử dụng quyền root cài qua Terminal hoặc sử dụng Synaptic Packet <giống như cái trình quản lý những ứng dụng đã cài đặt trong hệ thống> ^.^.
  + Cơ bản gồm 2 bước chính:
    - Cài đặt Snort:
      * Hiện tại bản plug-in IDMEF cho Snort chỉ hỗ trợ cao nhất đển version 2.8.x , tuy nhiên khi thử cài đặt với các bản 2.8.6 trở lên đều không tương thích , hiện sử dụng là bản Snort 2.8.3 <tuy nhiên hiện tại Snort không cung cấp source code của các bản snort cũ –hiện chỉ cung cấp v2.9- nên ta phải down từ các nguồn khác>
      * Khi cài đặt cần lưu ý:
        + Cần cài thêm “daq” down từ web chính của Snort <bản Snort cho win không cần cái này>
        + Nếu xuất hiện lỗi trong quá trình configure/make/make install lien quan đến file server\_stat.c , thì cần chỉnh sửa file này <xem đường dẫn khi thong báo lỗi xuất hiện> , cụ thể chỉnh sửa có thể search google có hướng dẫn cụ thể .
        + Khi cài plug-in này ,Snort cần sử dụng libtool <một thư viện> , tuy nhiên bản libtool khi cài mặc định là bản 2.x , bản này sẽ dẫn đến lỗi khi cài đặt , bởi vậy cần down libtool version 1.5 về , sau khi configure snort thành công , chép đè 2 file từ libtool 1.5 source code gồm :libtool và ltmain.sh ghi đè vào thư mục gốc của Snort đang config.
    - Cài đặt hệ thống rule tương ứng
      * Hiện tại Snort.org không cung cấp các gói rule ứng với các version snort cũ như 2.8.3 của chúng ta => buộc phải lấy nguồn từ internet .
      * Cần chạy script trong source code của IDMEF plugin tại thư mục chứa rule để chỉnh sửa các rule tương ứng.
      * Cần chỉnh sửa một số phần trong file snort.conf như:
      * Xuất output ra định dạng idmef:
        + Thêm dòng này:

output idmef: $HOME\_NET output=log dtd=idmef-message.dtd analyzerid=IDS1 indent=true facility\_default=file|idmef-messages.log alert\_id=/var/log/alert\_id\_num default=ascii.

* + - * Tùy chỉnh một số thong số rule không phù hợp :
        + Thêm # trước các file rule tương ứng <không sử dụng các gói rule này>

Trên đây chỉ là cơ bản sườn chính , tùy vào hệ thống mỗi người cài sẽ gặp những lỗi khác nhau , thêm nữa các trong các gói source code có các file hướng dẫn cụ thể các bước riêng nên không tiện liệt kê hết trong file này.