Samhain

1. Các hệ điều hành được hỗ trợ
   * Windows 2000/XP với POSIX emulation (Cygwin)
   * POSIX Linux
2. Cấu trúc hệ thống
   * Hoạt động riêng lẻ
   * Dạng client-server gồm các thành phần
     1. Client: samhain
        + Agent chạy ở phía host, có thể chạy ở dạng daemon
     2. Server: yule
        + Log server: thu thập log file từ nhiều agent
        + Có thể gửi các thông tin config thông qua runtime configuration file và thông tin về bảo mật qua baseline database
     3. Hệ cơ sở dữ liệu: hỗ trợ Oracle, MySQL, PostgreSQL. Có thể không sử dụng DB vẫn được
     4. Beltane: hỗ trợ báo cáo thông tin cho người dùng
        + Lấy report từ database, hiển thị lên để xem xét.
        + Hỗ trợ cập nhật baseline database
        + Sử dụng PHP
3. Một số tính năng trong việc kiểm tra tính toàn vẹn của các file trên hệ thống
   * Sử dụng Checksum, size, owner, ngày tạo, ngày sửa
   * Trên 1 số host dùng Linux có thể kiểm tra xem được ai sửa file (chức năng này chỉ được hỗ trợ trên 1 số kernel)
   * Samhain có thể thu thập thông tin về SELinux nếu chức năng này được hỗ trợ trên host đó(SELinux: 1 dạng MAC được hỗ trợ trên Linux)
   * Đối với 1 số file dung lượng nhỏ, có thể lưu file đó trong baseline DB để check thay đổi sau này
   * Có thể hỗ trợ schedule
4. Một số tính năng trong việc kiểm tra tính toàn vẹn của host
   * Phân tích logfile
     1. Hỗ trợ các dạng log của Linux (không thấy có của Windows!)
     2. Có khả năng correlate các sự kiện
   * Kiểm tra registry của Windows
   * Kiểm tra tính toàn vẹn của kernel đối với Linux (chống kernel rookits)
   * Có thể kiểm tra các process nào chạy nhưng ẩn.
   * Kiểm tra port nào đang mở
   * Các tác vụ logon/logoff
5. Một số lưu ý
   * Có thể sử dụng với prelude
   * Lisence GNU
6. Kết luận:
   * Có thể sử dụng với hệ thống mình đang xây dựng.