# Clam Antivirus

1. **Giới thiệu Clam Antivirus**

Clam AntiVirus [1] là một bộ công cụ chống virus mã nguồn mở (GPL), được thiêt kế đặc biệt cho việc chống virus ở các hệ thống thư điện tử. Clam AntiVirus cung cấp khá nhiều tiện ích bao gồm dịch vụ quét virus đa luồng (cung cấp dịch vụ quét virus cho các chương trình khác qua giao tiếp socket), bộ quét virus qua dòng lệnh và cập nhật dữ liệu virus tự động. Cốt lõi của gói công cụ là engine antivirus được cung cấp dưới dạng thư viện chia sẻ.

Clam Antivirus được nhiều tổ chức vừa và nhỏ dùng trong hệ thống thư điện tử của mình như:

* Chính quyền bang Vermont (Mỹ)
* Trường đại học Michigan (Mỹ)
* Trường đại học Nantes (Pháp)
* Webmail.us

1. **Cài đặt và sử dụng**
2. **Cài đặt**

Việc cài đặt chương trình Clam Antivirus tương đối đơn giản. Đối với các distro Linux Debian như Ubuntu, Debian… thì có thể cài đặt bằng lệnh:

*apt-get install clamav*

Trong trường hợp các distro RedHat như Fedora thì ta cài đặt bằng lệnh:

*yum install clamav*

Ngoài ra, còn có thể cài đặt Clam AntiVirus bằng cách tải bộ source code của Clam AntiVirus và tiến hành biên dịch, cài đặt trên máy. Quá trình cài đặt qua các bước như sau:

* Đăng nhập với quyền root, tạo user và group mang tên clamav

*groupadd clamav*

*useradd –g clamav –s /bin/false –c "Clam AntiVirus" clamav*

* Cấu hình cho trình biên dịch, trước hết cần phải chuyển thư mục làm việc đến thư mục source code của Clam Antivirus, sau đó chạy lệnh:

*./configure*

Chương trình sẽ kiểm tra các gói cần thiết cho việc biên dịch đã được cài đặt chưa, nếu chưa thì cần phải cài đặt theo thông báo mà trình *configure* đưa ra.

* Sau khi quá trình cấu hình hoàn tất, ta bắt đầu biên dịch chương trình:

*make*

* Sau đó là cài đặt chương trình vào máy tính:

*make install*

1. **Sử dụng**

Clam AntiVirus cung cấp bốn công cụ chính đó là:

* clamd: chương trình chạy thường trú trong hệ thống, cung cấp dịch vụ quét virus cho các chương trình khác qua giao tiếp socket, có thể là UNIX local socket hoặc TCP socket. Cách thức hoạt động của *clamd* được cấu hình trong file *clamd.conf.* Sau khi đã tạo được kết nối với *clamd*, ta có thể dùng các lệnh sau để điều khiển *clamd*:
  + PING (kiểm tra trạng thái hoạt động của *clamd*, *clamd* sẽ trả lời lại là PONG)
  + RELOAD (nạp lại dữ liệu virus)
  + SHUTDOWN (thoát chương trình)
  + SCAN file/thư mục (quét file/thư mục)
  + MULTISCAN file/thư mục (quét file theo phương pháp chuẩn hoặc dùng nhiều luồng để quét đệ quy thư mục)
  + INSTREAM (quét một dòng dữ liệu, dữ liệu sẽ được truyền qua giao tiếp socket đã được kết nối)
* clamdscan: đây là một client đơn giản dùng để giao tiếp với *clamd*, *clamdscan* chấp nhận các tùy chọn quét như *clamscan* nhưng các tùy chọn này phải được *clamd* chấp nhận bằng việc tinh chỉnh cấu hình trong file *clamd.conf*.
* clamscan: chương trình quét virus chạy trực tiếp bằng dòng lệnh, độc lập với *clamd*. Một số ví dụ đơn giản sử dụng *clamscan*:
  + clamscan file (quét file)
  + clamscan –r directory (quét tất cả các file và thư mục con của directory)

Ngoài ra, *clamscan*  còn cho phép tùy chọn tắt hay mở các quy trình quét như:

* --phishing-scan-urls[=yes(\*)/no]: mở/tắt module phát hiện phishing
* --algorithmic-detection[=yes(\*)/no]: mở/tắt module phát hiện các virus phức tạp dùng các giải thuật phân tích
* --scan-pe[=yes(\*)/no]: mở/tắt module quét file thực thi
* --scan-archive[=yes(\*)/no]: mở/tắt module quét file nén
* freshclam: là trình cập nhật dữ liệu virus cho Clam AntiVirus, có hai chế độ hoạt động:
  + Chỉ cập nhật virus mỗi khi được người dùng chạy chương trình:

*freshclam*

* Chạy thường trú trong hệ thống và tự động cập nhật dữ liệu:

*freshclam –d*

Các cấu hình hoạt động của *freshclam* được lưu trong file cấu hình *freshclam.conf*.

1. **Dữ liệu virus**

Dữ liệu virus chính của Clam AntiVirus được lưu trong file *main.cvd*. File *main.cvd* này sẽ được cập nhật ở mỗi phiên bản mới của Clam AntiVirus. Trong quá trình sử dụng, người dùng muốn cập nhật dữ liệu virus có thể dùng chương trình *freshclam,* chương trình này sẽ dựa vào phiên bản của dữ liệu hiện thời và tải các dữ liệu mới hơn, lưu vào file *daily.cvd*. Ta có thể kiểm tra phiên bản hiện thời của file *.cvd* bằng cách dùng chương trình *sigtool* như sau:

s*igtool –info “file .cvd”*

Ví dụ với file *main.cvd*:

*sigtool –info main.cvd*

*File: main.cvd*

*Build time: 15 Feb 2010 09:54 -0500*

*Version: 52*

*Signatures: 704727*

*Functionality level: 44*

*Builder: sven*

*MD5: 59b7133605b0857b1a76bfe8b3645ff5*

*Digital signature: +FudokGFjmVwPvarlZwGalZIOon/HuOUKiadDgb9SkbQk/dwx2gGZjko04g6X+uurBuGqlLfUs6/gLMtCcxCHwolU6BEDKj2WLQE0OOwXnNMbE7JCxSHh/zAIQVJ/pHcSkNdSsqFyayjFO4ShSf4rTFzYJkmvOV0zI5/eZbv2b*

*Verification OK.*

File *.cvd*  là một tập hợp các file dữ liệu nhỏ hơn. Dùng trình *sigtool* ta có thể giải nén các file này:

s*igtool –u file.cvd*

Mỗi file được giải nén ra sẽ là một danh sách các mẫu virus . Mẫu virus ở mỗi file có định dạng khác nhau, Clam AntiVirus sẽ căn cứ vào tên file để xác định phương pháp đọc mẫu thích hợp.

* File *.hdb*: chứa các giá trị hash MD5 của các mẫu virus đã phát hiện được

Đây là ví dụ một mẫu trong file *main.hdb*

Giá trị hash MD5

Tên virus

2401851daa0343df8ff683f730fec39:92281:Dialer-85

Kích thước file

Để tạo một mẫu virus MD5 cho một file bất kì, ta dùng chương trình *sigtool* như sau:

s*igtool –md5 file*

Ví dụ*:*

*sigtool --md5 test.exe*

ta được kết quả:

*48c4533230e1ae1c118c741c0db19dfb:17387:test.exe*

* File *.mdb*: chứa giá trị hash MD5 của PE section trong một file nhiễm virus.

Mẫu virus này có dạng:

Tên virus

Kích thước section

7168:a105e2cc8148158cd048360eb847c7d0:Trojan.Downloader-1421

Giá trị hash MD5

Cách dễ nhất để tạo mẫu virus PE section này là tách các sections của file ra từng file rồi biệt rồi dùng trình *sigtool*  với tùy chọn chọn là *–mdb*.

* File *.db*: chứa nội dung của mẫu virus biểu diễn dưới dạng chuỗi hex.

Mẫu virus này có dạng:

Biểu diễn hex của file

Tên virus

\_0017\_0001\_000=21b8004233c999cd218bd6b90300b440cd218b4c198b541bb80157cd

Mẫu virus này được tạo bằng cách dùng lệnh như sau:

*cat virusfile | sigtool –hex-dump*

* File *.ndb*: các mẫu virus dạng chuỗi hex mở rộng với các thông tin thêm về dạng file, offset mà tại đó bắt đầu chuỗi nhận dạng.

Biểu diễn hex của chuỗi nhận dạng

Tên virus

Offset

Trojan.Small-3667:1:EP+0:b82196e70f2d2164a50f5050e8??000000e8

Dạng file

1. **Qui trình quét virus của Clam Antivirus**

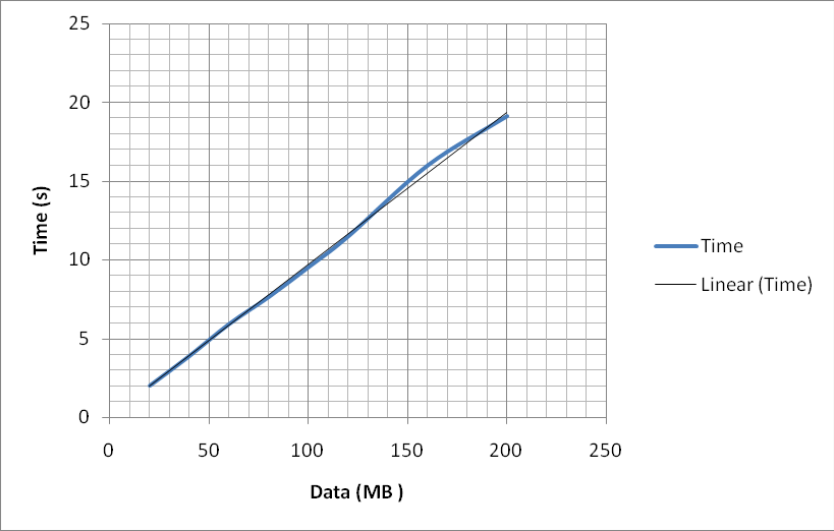
Hình 1 mô tả các bước thực hiện một qui trình quét virus của Clam Antivirus.



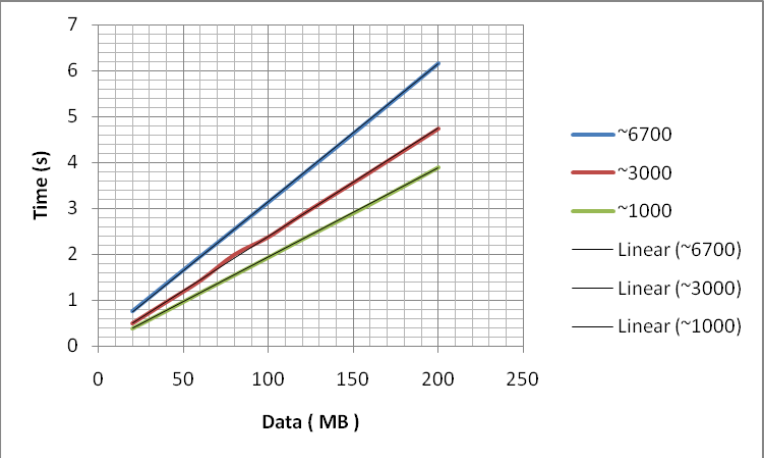
*Hình 1 - Sơ đồ qui trình quét virus của Clam Antivirus*

1. **Kết quả hoạt động chương trình ClamAV**

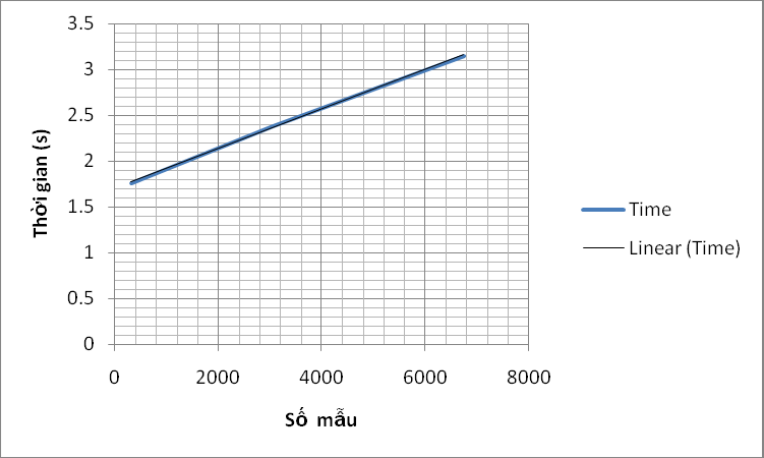
* Test ClamAV với số mẫu nhận dang là 1054224



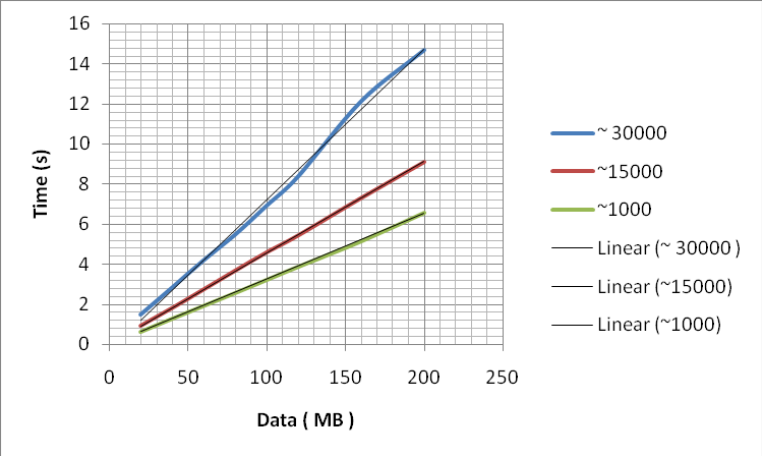
* Test AC khối lượng quét thay đổi, các đường biểu diễn số mẫu khác nhau



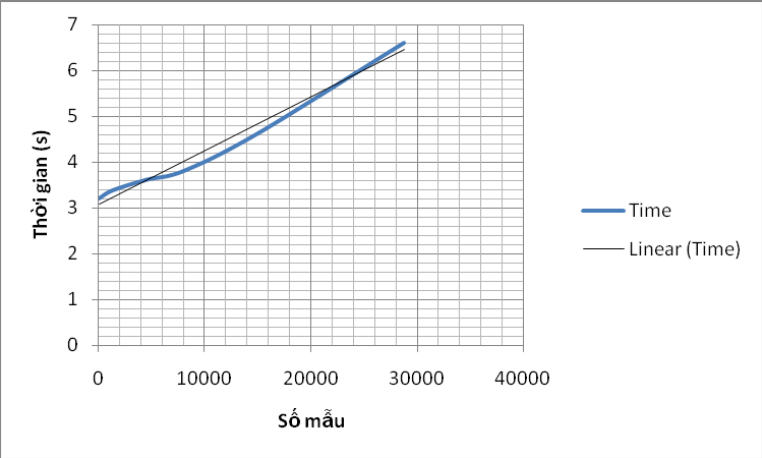
* Test AC với Data là 100MB, số mẫu thay đổi



* Test BM khối lượng quét thay đổi, các đường biểu diễn số mẫu khác nhau



* Test BM với Data là 100MB, số mẫu khác nhau



Điều kiện thử nghiệm

* CPU : Dual core 1.6GHz
* Ram : 2Gb
* OS : Ubuntu 10.10

Trong quá trình kiểm nghiệm, hệ thống ở trạng thái không tải, CPU ~ 2-3%. Khi ClamAV tiến hành quét, CPU khá ổn định ở 50%, do ClamAV chỉ có thể chạy trên 1 lõi.