**I. Hướng dẫn sử dụng công cụ**

**Yêu cầu:**

* Phiên bản hệ điều hành tối thiểu: CentOS 7.0, Oracle Linux 7.0, Fedora 19, Ubuntu 13.10, Debian 8 (Jessie), RHEL 7.0, SUSE Linux Enterprise Server 12, Windows 7 64bit.

Nếu server không đáp ứng được phiên bản tối thiểu, có thể tiến hành cài đặt công cụ trên một máy trung gian, sau đó tiến hành sao chép mã nguồn và dữ liệu từ server về để tiến hành rà quét.

**Hướng dẫn sử dụng:**

Tải về công cụ bằng câu lệnh sau, sử dụng tài khoản bitbucket đã được cấp phép mới có thể truy cập được:

git clone https://bitbucket.vnptmedia.vn/scm/~quanphamngoc/webshell-scan.git

Lưu ý: Nếu không truy cập được đường dẫn, vui lòng liên hệ TT.ANTT để được thêm quyền truy cập.

**Đối với Windows:**

Tiến hành rà quét, tại thư mục webshell-scan vừa tải về, mở command-line với quyền administrator:

**webshell-scan.exe -p path-to-folder -o log-file.log**

Trong đó:

- path-to-folder là đường dẫn tuyệt đối tới folder nơi chứa dữ liệu cần rà quét

- log-file.log là tên của file log, có thể đặt tên tuỳ ý

**Đối với Linux:**

Tại thư mục webshell-scan vừa tải về, mở terminal với quyền root:

Tiến hành cấp quyền thực thi cho file webshell-scan:

**chmod 700 webshell-scan**

Tiến hành rà quét, thực hiện câu lệnh sau:

./**webshell-scan -p path-to-folder -o log-file.log**

Trong đó:

- path-to-folder là đường dẫn tuyệt đối tới folder nơi chứa dữ liệu cần rà quét

- log-file.log là tên của file log, có thể đặt tên tuỳ ý

**Sau khi tiến trình rà quét hoàn thành:**

* Sau khi rà quét hoàn thành, file log sẽ được tạo ra ở trong thư mục logs trong thư mục webshell-scan gồm 2 file .log và .xlsx
* File log có cấu trúc như sau:
  + FILE: đường dẫn tới file
  + SCORE: điểm đánh giá mức độ nguy hiểm
  + TIME (CREATED, MODIFIED, ACCESSED): ngày khởi tạo, thay đổi, truy cập của file
  + DESCRIPTION (REASON\_x): mô tả
* **File log này phải được gửi cho dev để kiểm tra từng file trước khi tiến hành xoá bỏ tránh tình trạng nhầm lẫn với file hệ thống.**