**Tài liệu hướng dẫn công cụ webshell\_scan**

1. Cài đặt các package Python cần thiết:

* Trên Windows:

pip install configparser pysmb requests psutil pywin32

* Trên Linux:

pip install configparser pysmb requests psutil crontab croniter

1. Cách biên dịch chương trình

* Cài đặt pyinstaller:

pip install pyinstaller

* Thêm đường dẫn thư mục chứa pyinstaller vào biến môi trường PATH: (Chỉ yêu cầu trên Windows)

C:\Users\<username>\AppData\Local\Programs\Python\Python39\Scripts

* Build chương trình:

pyinstaller <options> webshell\_scan.py

* + --upx-dir: đường dẫn tới thư mục chứa công cụ UPX Packer
  + -D: build dưới dạng 1 thư mục
  + -F: build thành 1 file thực thi duy nhất

1. Cách sử dụng công cụ webshell\_scan

* Đặt file config.conf vào cùng thư mục với file thực thi (.exe) hoặc file mã nguồn (.py)
* Kiểm tra các mục cấu hình trong mục [config]:
  + dir: đường dẫn tuyệt đối đến thư mục cần scan. Có thể gồm nhiều đường dẫn khác nhau, các đường dẫn được phân cách bởi dấu “,”

Ngoài các thư mục được người dùng định nghĩa trong mục “dir” trên, mặc định các thư mục sau sẽ được quét thêm:

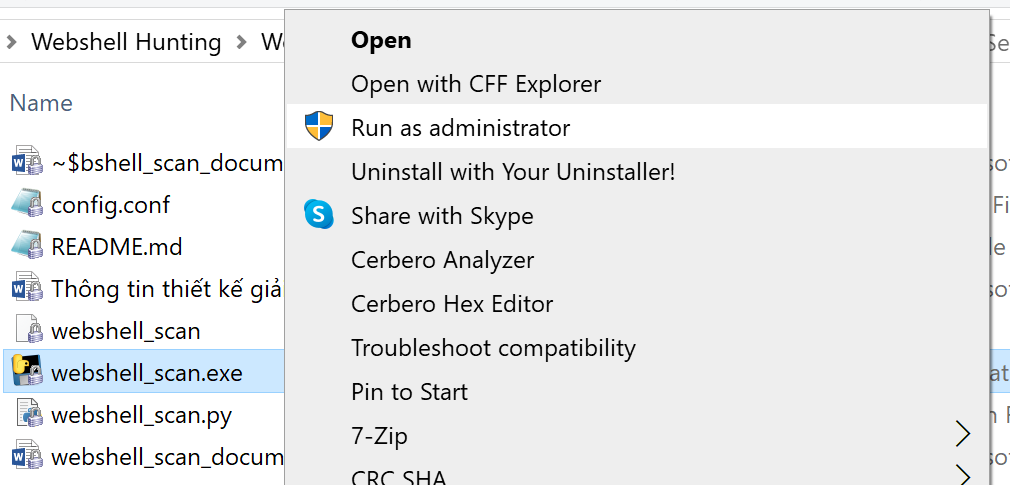
* Trên Windows:
  + C:\xampp\htdocs\
  + C:\inetpub\wwwroot\
  + c:\Apache24\htdocs\
* Trên Linux:
* /var/www/html
* /var/http/
* /srv/http/
* /etc/apache2/
* /etc/nginx/
* /etc/httpd/
* /usr/local/apache2
* /webapps/ROOT/
* /applications/DefaultWebApp/
* /opt/lampp/httpdocs/
  + domain: domain của từng thư mục web được scan. Cần có số lượng bằng với số thư mục scan đã được xác định trong mục dir
  + database: địa chỉ web của file database chứa thông tin các file đã scan (file .json chứa thông tin file blacklist và whitelist)
  + size: quy định kích thước tối đa của file được scan. Chương trình sẽ không quét các file kích thước > size
  + ext: quy định các định dạng file được scan. Các định dạng file cần được ngăn cách bởi kí tự “|”. Mặc định là tất cả các định dạng webshell phổ biến (.php|.asp|.aspx|.sh|.bash|.zsh|.csh|.tsch|.pl|.py|.cgi|.cfm|.jsp|.htaccess|.ashx|.vbs|.ps1|.war|.js|.jar).
  + crontab: Chỉ yêu cầu với Linux. Xác định lịch thực thi chương trình webshell scan dựa trên crontab. Yêu cầu cần đặt giá trị đúng định dạng crontab. Mặc định giá trị là "0 0 1 \* \*" (ngày đầu tiên của tháng)
  + days\_interval: Chỉ yêu cầu với Windows. Xác định lịch thực thi chương trình webshell scan dựa trên Task Scheduler. Mặc định giá trị là 30 (sau 30 ngày sẽ thực hiện quét 1 lần)
* Chạy chương trình:
  + Từ mã nguồn: **Cần chạy với quyền Administrator (Windows)**

python webshell\_scan.py

* + Từ file thực thi (Windows): **Cần chạy với quyền Administrator**
    - C1: Mở cửa sổ CMD (được Run as adminstrator), chuyển đến thư mục chứa chương trình và gõ lệnh

.\webshell\_scan.exe

* + - C2: Chuột phải vào chương trình webshell\_scan.exe, chọn Run as administrator.



* + Từ file thực thi (Linux): Mở cửa sổ Terminal, chuyển đến thư mục chứa chương trình và gõ lệnh:

./webshell\_scan

1. Lưu ý:

* Nếu muốn build file thực thi trên các môi trường khác nhau, ứng với nền tảng x86 hoặc x64, cần thực hiện chạy pyinstaller trên môi trường tương ứng.
* Nếu quá trình cài đặt các gói bằng pip xảy ra lỗi:

There was a problem confirming the ssl certificate: HTTPSConnectionPool(host='pypi.org', port=443)

Thì sử dụng câu lệnh sau để cài đặt các gói:

pip install --trusted-host pypi.org --trusted-host files.pythonhosted.org <package\_name>