CÔNG CỤ NIKTO

Nikto là một phần mềm mã nguồn mở được sử dụng kiểm tra các vấn đề bảo mật của Web Server bằng một hệ thống cơ sở dữ liệu riêng đến khoảng 70 ngàn lỗi bảo mật thông thường được tìm thấy và cập nhật với từng phiên bản.

Nikto có thể hoạt động trên các hệ điều hành cơ bản:

- Windows
- Linux
- Mac OS

Các chức năng mà Nikto có thể thực hiện:

- Tìm SQL injection, XSS và các lỗ hổng phổ biến khác
- Xác định phần mềm đã cài đặt (thông qua tiêu đề, biểu tượng yêu thích và tệp)
- Đoán tên miền phụ
- Bao gồm hỗ trợ cho các trang web SSL (HTTPS)
- Lưu báo cáo ở dạng văn bản thuần túy, XML, HTML hoặc CSV
- Báo cáo các tiêu đề bất thường
- Kiểm tra các mục cấu hình máy chủ như nhiều tệp chỉ mục, tùy chọn máy chủ HTTP, v.v.
- Có hỗ trợ proxy HTTP đầy đủ
- Đoán thông tin đăng nhập để ủy quyền (bao gồm nhiều tổ hợp tên người dùng / mật khẩu mặc định)
- Được định cấu hình với công cụ mẫu để dễ dàng tùy chỉnh báo cáo

Các lệnh cơ bản Nikto:

- Quét miền

  ```
  > nikto -h scanme.nmap.org
  ```

- Quét miền có SSL được bật

  ```
  > nikto -h https://nmap.org –ssl
  ```

- Quét địa chỉ IP

  ```
  > nikto -h IP
  ```

- Quét và xuất kết quả quét:

  ```
  > nikto -h scanme.nmap.org -o scan.txt
  ```

nikto cheat sheet

comparitech

Installation	$ sudo apt-get install nikto

Standard command to scan websites	nikto -host (web url host name) -(http port number)

Scan options

Nikto -h (Hostname /IP address)	Quét 1 máy chủ
Nikto -h -port (Port Number1),(Port Number2)	Quét máy chủ sử dụng cổng cụ thể
Nikto -h (Hostname) -maxtime (seconds)	Thời gian quét tối đa
Nikto -h-until	Khoản thời gian để quét
Nikto -h-vhost	Xác định header của máy chủ
Nikto -h-no404	Bỏ qua http 404
Nikto -h-nossl	Không dùng SSL khi quét
Nikto -h-ssl	Dùng SSL khi quét
Nikto -update	Cập nhật Nikto
Nikto -h-dbcheck	Kiểm tra cơ sở dữ liệu
Nikto -h (Hostname/IP address) -output (filename)	Lưu kết quả thành 1 file
Nikto -h-useproxy (Proxy IP address)	Quét máy chủ web thông qua proxy
Nikto -h-config (filename.conf)	Dùng 1 file để làm cơ sở dữ liệu
Nikto -h-nolookup	Dừng DNS loopkup đối với các máy chủ
Nikto -h-nocache	Dừng caching responses khi quét

Display Options

Nikto -h -Display (option)

1	Hiển thị các điều hướng
2	Hiển thị cookies
3	Hiển thị phản hồi 200 ok
4	Hiển thị Web URLs yêu cầu xác thực
D	Hiển thị debug
E	Hiện HTTP errors
P	In thành dữ liệu STDOUT
V	Hiện thị chi tiết đầu ra

Output Options

Nikto -h -Format

csv	Comma Separated Value
htm	Định dạng HTML
txt	Định dạng text
xml	Định dạng XML

Tuning Options

Nikto -h (Hostname) -tuning (Option)

0	Lỗi upload file	7	Truy xuất file từ xa thông qua server
1	Xem chi tiết file của log	8	Command Execution / Remote Shell
2	Sai sót cấu hình file	9	Tiêm nhiễm SQL
3	Hiển thị thông tin công khai	a	Bypass cơ chế xác thực
4	Tiêm nhiễm (XSS/Script/HTML)	b	Nhận dạng phần mềm
5	Truy xuất file từ xa thông qua web root	c	Remote Source Inclusion
6	Từ chối dịch vụ	x	Reverse Tuning Options

Reference and additional resources - https://github.com/sullo/nikto