MÔ HÌNH TẠO BÁO CÁO QUÉT KẾT QUẢ QUÉT FILE

\*Tổng quan: Mô hình này cho phép 1 máy thu nhận các kết quả quét file từ 2 phần mềm Anti-virus sau đó hiển thị lên dạng web.

**1) Thành phần trong mô hình**

|  |  |  |
| --- | --- | --- |
| **Host** | **IP address** | **Port** |
| Web Server (Kali Linux) | 10.81.36.5 | 5000,8000 |
| Engine Kaspersky (Windows 10 HAU-DC) | 10.81.36.10 | 9999 |
| Engine Windows Defender (Windows 10 ZECTER) | 10.81.36.30 | 9999 |

**2) Cấu hình**

Engine Kaspersky được bật chế độ thu động để quét file qua command line bằng công cụ “C:\Program Files (x86)\Kaspersky Lab\Kaspersky 21.18\avp.com”

Vd: avp.com SCAN “C:\Users\HAU-DC\virus.exe” /RA:“C:\Users\HAU-DC\report.txt”

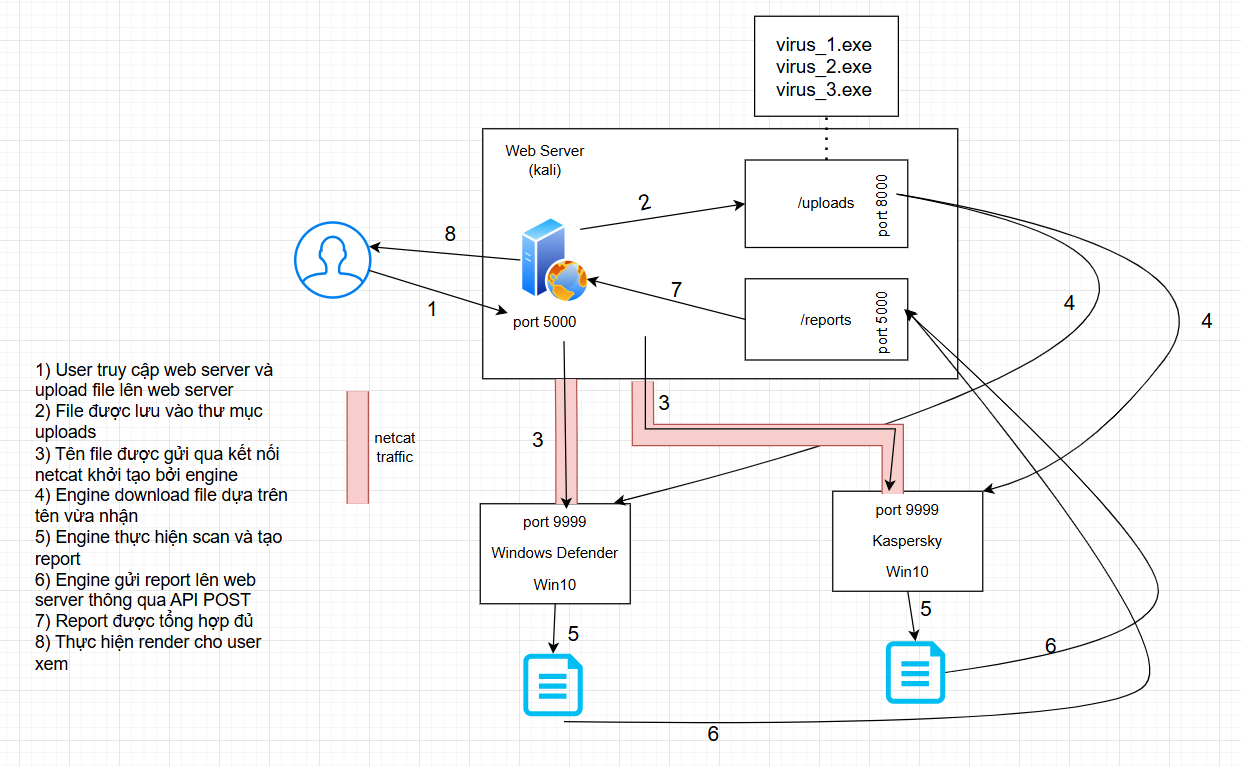
/RA: để tạo report

Engine Windows Defender được bật chế thu động để quét file qua command line bằng công cụ “C:\Program Files\Windows Defender\MpCmdRun.exe"

Vd: MpCmdRun.exe -Scan -ScanType 3 -File “C:\Users\HAU-DC\virus.exe”

Để có thể lấy report của Engine Windows Defender, ta sử dụng command “ Get-WinEvent -LogName “Microsoft-Windows-Windows Defender/Operational” | Where-Object { $\_.Id -eq 1116 } | Select-Object Message | Select-String -Pattern “tên-file” ”

**3) Mô hình tổng quát**



- Bước 1: Upload File

Thực hiện upload file lên trang web