1) Triển khai virus scan engine

\*Microsoft Defender

- Cấu hình:

Ở mục “Virus & threat protection”, tắt “Tamper Protection”

Ở mục “App & browser”, chọn “off” với mỗi mục cấu hình

- Sử dụng command line: sử dụng “MpCmdRun.exe” trong “C:\Program Files\Windows Defender”

\*Kaspersky:

- Cấu hình:

Ở mục “General”, tắt “*Perform recommended actions automatically”*

Ở mục “Protection”, tắt tất cả options …

- Sử dụng command line: sử dụng “avp.com” trong “C:\Program Files (x86)\Kaspersky Lab\Kaspersky 21.18”

\*BitDefender

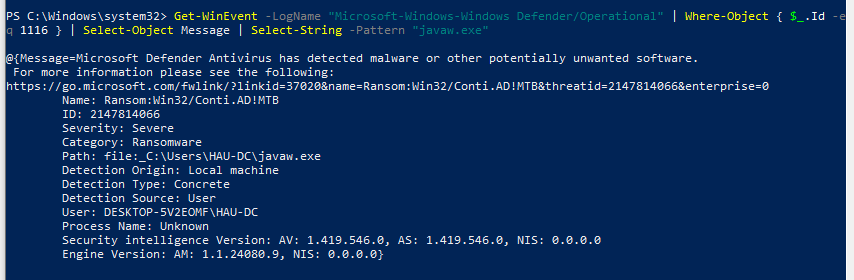
\*Avast

2) Thực hiện scan

\*Windows Defender

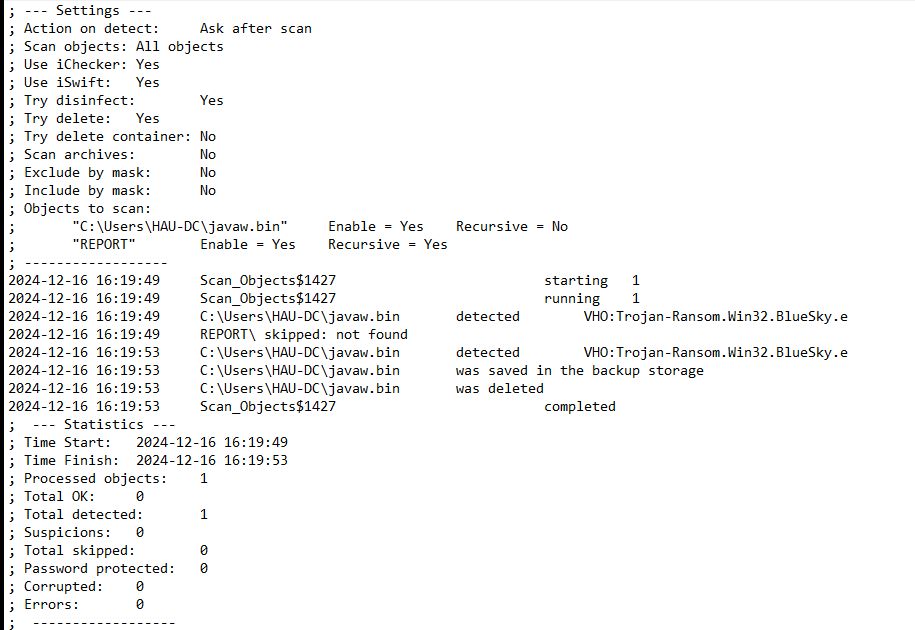
MpCmdRun.exe -Scan -ScanType 3 -File "C:\path\to\file"

Get-WinEvent -LogName “Microsoft-Windows-Windows Defender/Operational” | Where-Object { $\_.Id -eq 1116 } | Select-Object Message | Select-String -Pattern “javaw.exe”



\*Kaspersky

./avp.com SCAN /R:“C:\Users\HAU-DC\Documents\report.txt” “C:\path\_to\_file”



\* Mô hình triển khai

Sử dụng docker triển khai các Scan Engine bao gồm

1) Kaskpersky

2) Windows Defender

3) ClamAV docker

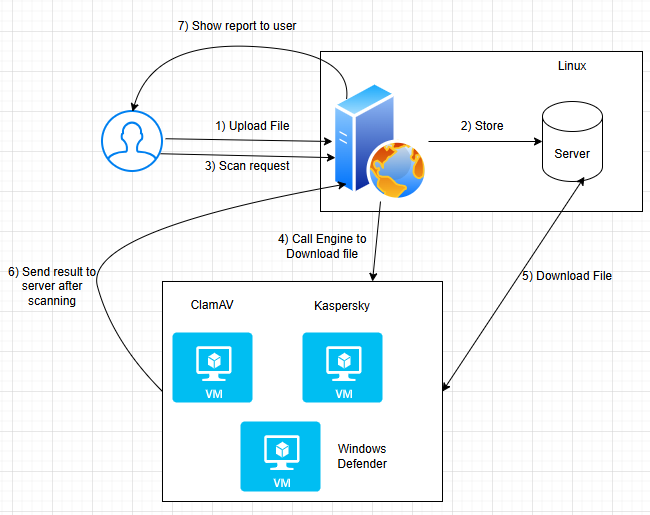
\*Giao diện web gồm:

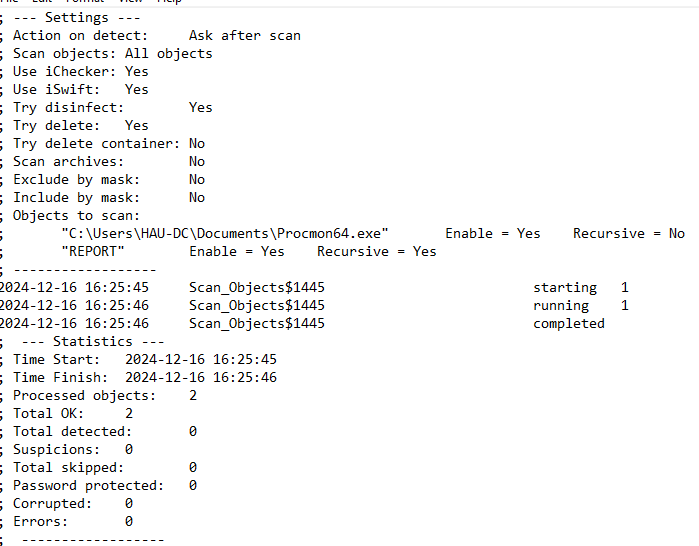
- Upload File

- Hiển thị upload file thành công / thất bại

- Tải file về engine

- Lấy kết quả scan và hiển thị lên web





\*Build dự án

dotnet publish -c Release -r win-x64 --self-contained true /p:PublishSingleFile=true

\*

; --- Settings ---

; Action on detect: Ask after scan

; Scan objects: All objects

; Use iChecker: Yes

;Try delete: Yes

; "D:\Code\test.txt" Enable = Yes Recursive = No

2024-12-25 16:12:40

2024-12-25 16:12:45 D:\Code\virus.txt detected VHO:Trojan-Ransom.Win32.BlueSky.e

2024-12-25 16:12:50

2024-12-25 16:13:20 D:\Code\virus.txt was delected

go.moircorsor.com?linkid=12345&name=Ransom

Name: Ransom:Win32/Conti.AD!MTB

ID: 2e242e2

-----------------------------274487903134313490382707725948

Content-Disposition: form-data; name="file"; filename="passwords.txt"

Content-Type: text/plain

password

pass

admin

msfpassword

metasploit

msfadmin

doordonot

-----------------------------274487903134313490382707725948—

POST /upload HTTP/1.1

Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7f59d872-553c-422a-af96-d687c26a029d

User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.5247

Host: 10.81.36.5:5000

Content-Length: 246

Connection: Keep-Alive

------WebKitFormBoundary7f59d872-553c-422a-af96-d687c26a029d

Content-Disposition: form-data; name="file"; filename="Kaspersky\_report\_1.txt"

Content-Type: text/plain

no virus

------WebKitFormBoundary7f59d872-553c-422a-af96-d687c26a029d--

HTTP/1.1 500 INTERNAL SERVER ERROR

Server: Werkzeug/2.3.8 Python/3.12.8

Date: Wed, 18 Dec 2024 16:35:09 GMT

Content-Type: application/json

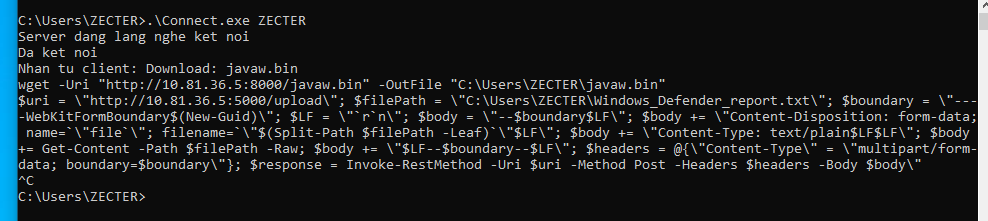
Content-Length: 34

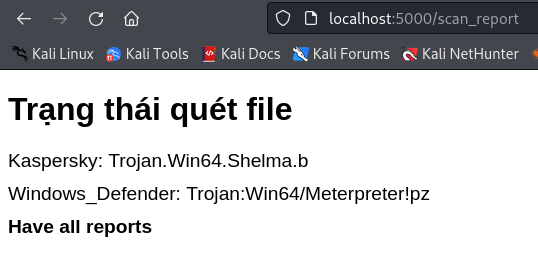
Connection: close

{

"error": "'REPORTS\_FOLDER'"

}







Strelka – Scan file

gRPC: giao thức truyền thông nhanh, nội bộ, gọi giữa các ứng dụng, sử dụng protobuf

Redis: cơ sở dữ liệu có khả năng truy cập nhanh từ cache, RAM, sử dụng key-value data

