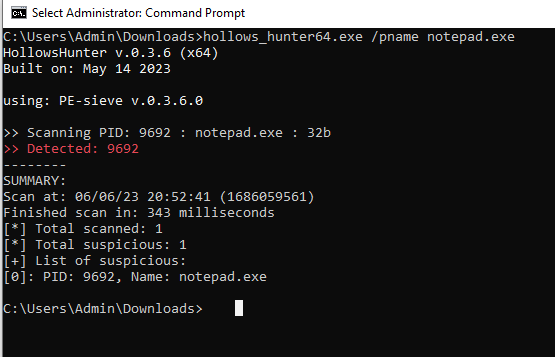
<https://github.com/hasherezade/hollows_hunter>

hollows hunter là tool giúp phát hiện các tiến trình bị inject code

tương tự các bài báo cáo trước ở đây em chạy chương trình process\_hollowing.exe với mục đích là inject code vào tiến trình notepad.exe



Hollows\_hunter đã phát hiện và đưa ra kết quả

Ưu điểm của tool này là ngoài phát hiện ra tiến trình bị inject code vào thì tool này còn dump được ra file

File này tuy không thực thi được nhưng load vào IDA thì có thể đọc được mã nguồn của chương trình ( thử với 1 số con mã độc khác thì file dump ra có khi không đọc được)