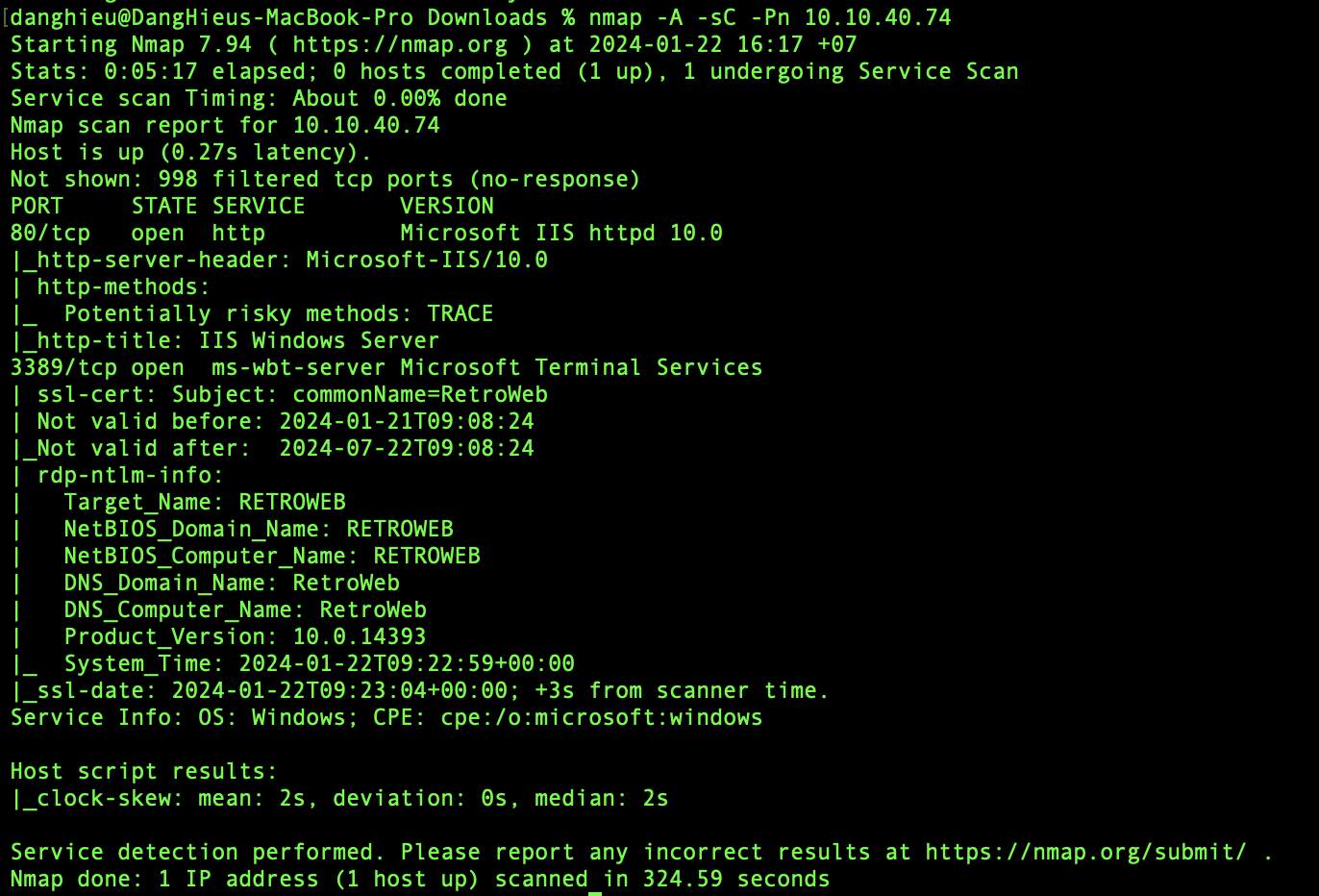
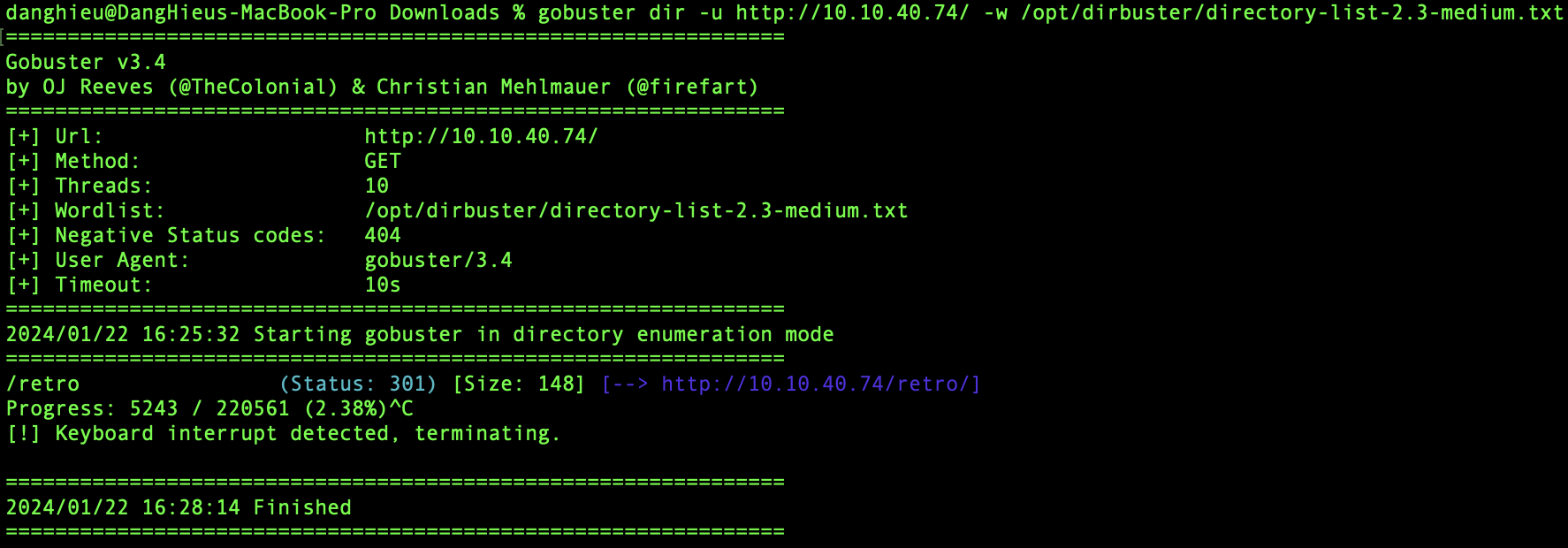
**Active Forward Scanners and Launch Proton Torpedoes**





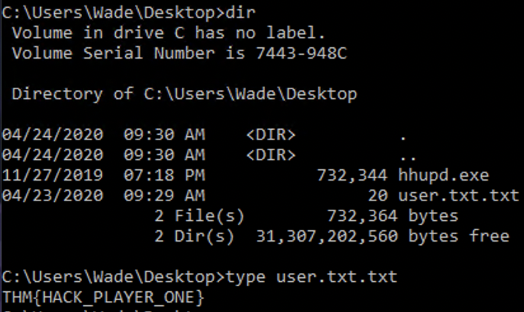
Giao diện của trang web là 1 trò chơi. Ta khám phá được tên của một người dùng: Wade

Mật khẩu tiềm năng của anh ấy là: parzival

Đăng nhập vào máy ảo qua Microsoft Remote Desktop

Màn hình desktop của wade:





**Breaching the Control Room**

Chúng ta đã giành được quyền truy cập vào hệ thống. Hãy thăm dò xung quanh để xem liệu chúng ta có tìm được điều gì thú vị trên hệ thống không.

Khi liệt kê 1 máy ảo, tìm xem người dùng đã làm gì vào lần cuối rất hữu ích. Liệu bạn có thể tìm thấy CVE nào đã được nghiên cứu trên máy chủ không?

Trong internet explorer, bạn kiểm tra lịch sử duyệt web của Dark, 2 tuần trước anh ấy có nghiên cứu cve-2019-1388

Tệp thực thi để khai thác lỗ hổng này, người dùng đã không dọn dẹp cẩn thận sau khi kiểm thử: hhupd.exe

**Case Study: CVE-2019-1388 Abuse UAC Windows Certificate Dialog**

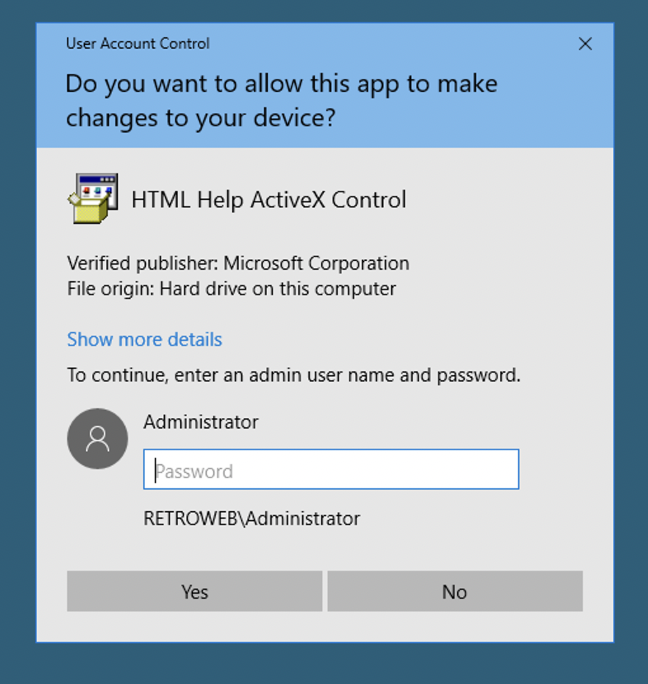
Mô tả: Khai thác này lạm dụng UAC windows Certificate Dialog để thực thi certificate issuer link (liên kết cấp chứng chỉ) với tư cách là NT Authority User và mở 1 trình duyệt dưới đặc quyền của NT Authority User. Sau đó ta có thể dùng điểu này để mở 1 shell với đặc quyền của NT Authority User

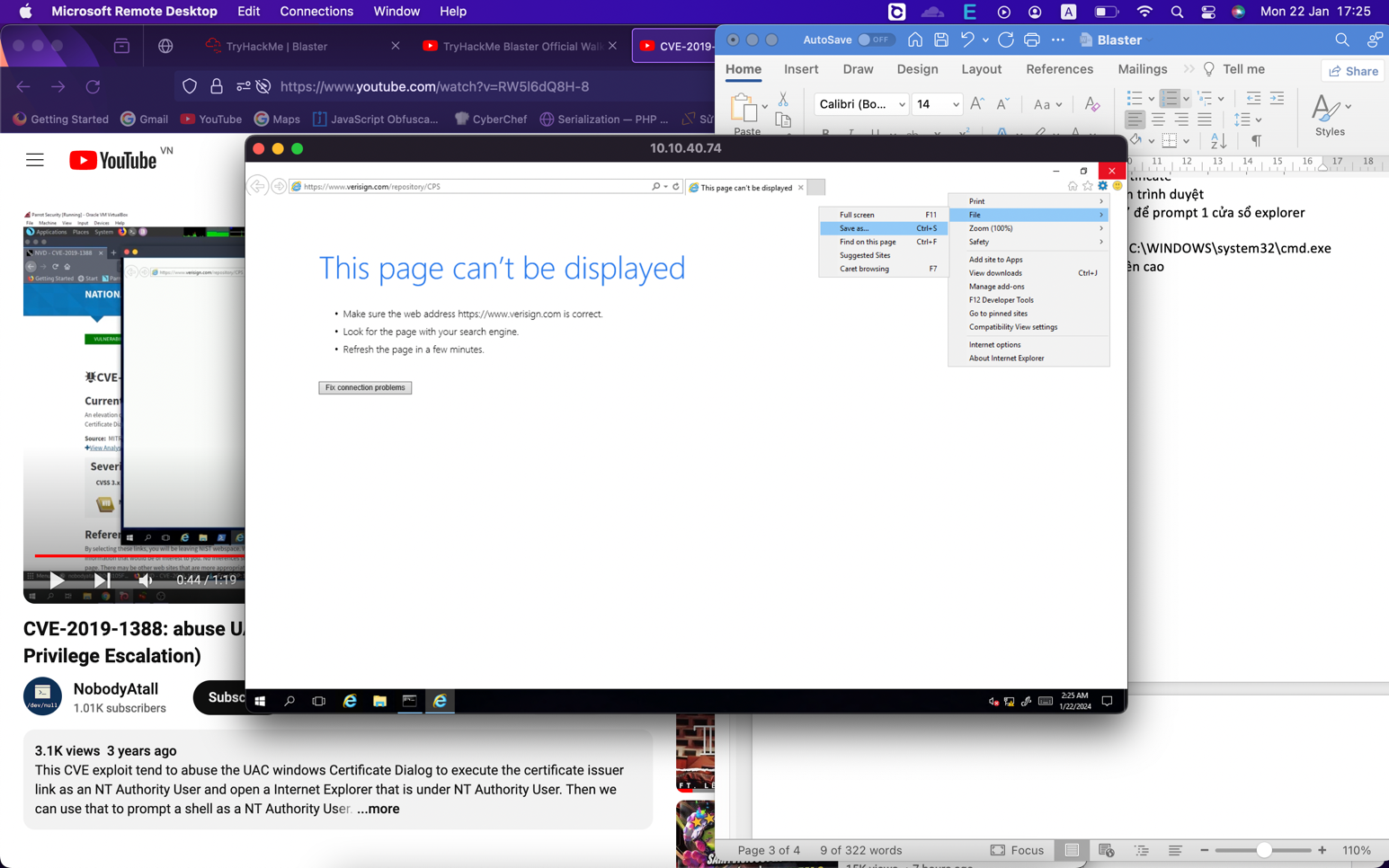
**Các bước:**

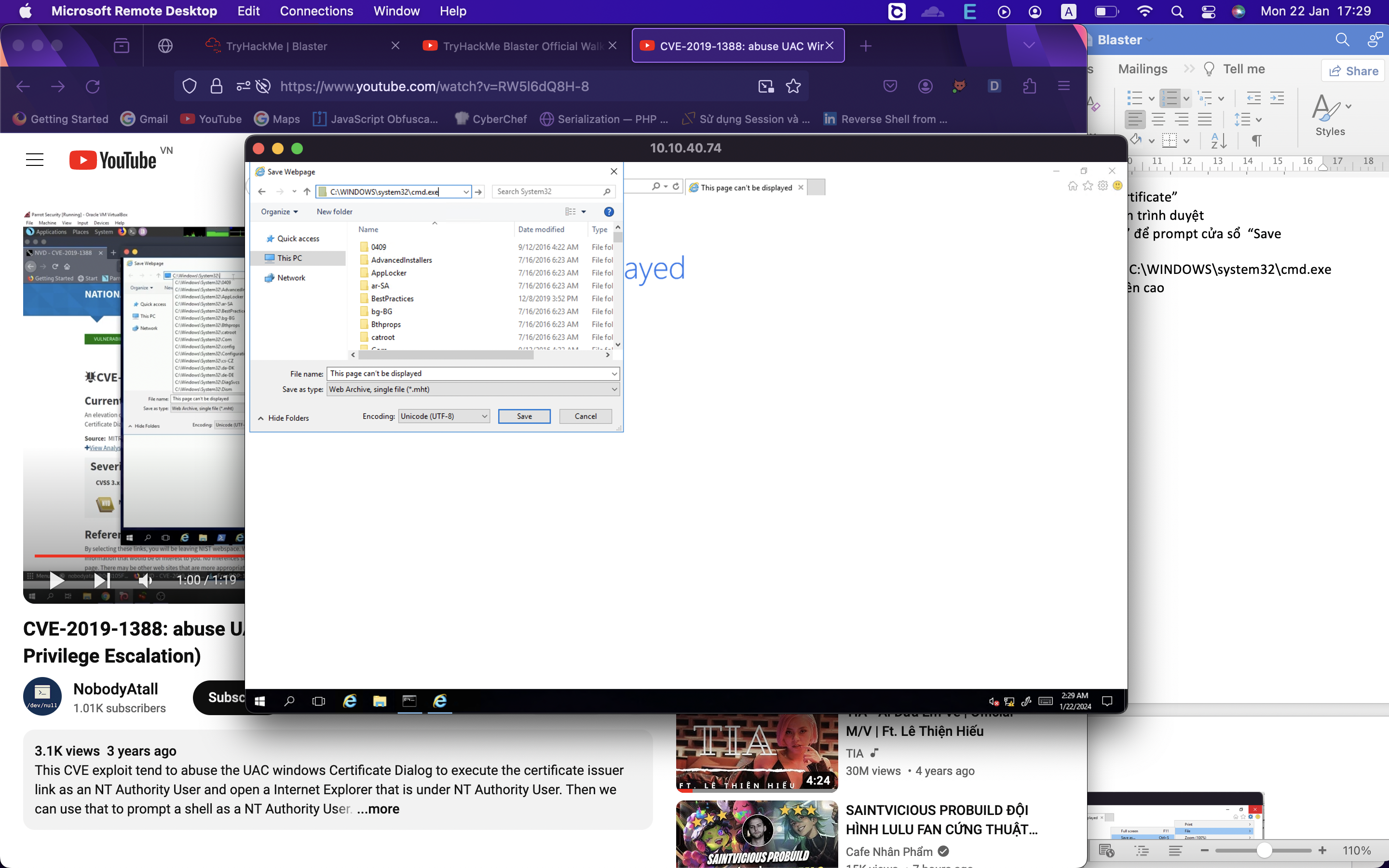
1. Tìm kiếm 1 chương trình có thể thực thi UAC prompt screen
2. Chọn “Show more details”
3. Chọn “Show information about the publisher’s certificate”
4. Chọn “Issued by” Url link, nó sẽ prompt 1 giao diện trình duyệt
5. Đợi trang web được tải hoàn tất và chọn “save as” để prompt cửa sổ “Save Webpage”
6. Trên explorer window, nhập đường dẫn cmd.exe: C:\WINDOWS\system32\cmd.exe🡪Enter
7. Bây giờ bạn đã có 1 command prompt có đặc quyền cao

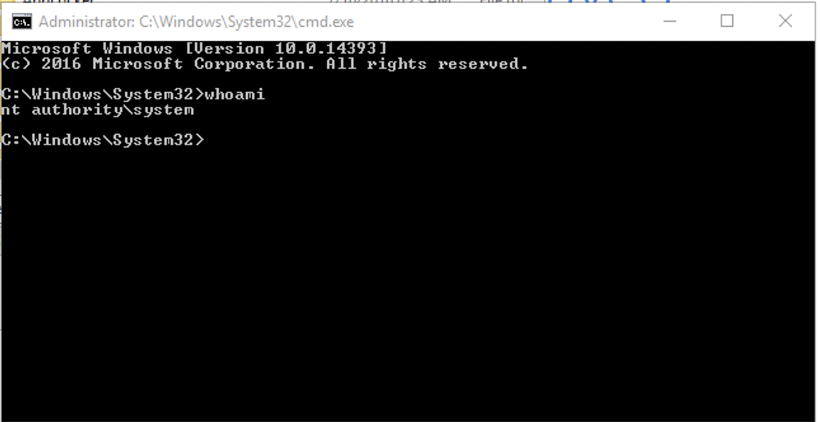
**Khai thác**

Chọn ứng dụng hhupd.exe









Cách tìm kiếm file:

