Lab giải thử thách CTF.

Chuẩn bị

- Tài khoản đăng nhập vào trang web cyberdefenders.org.
- Công cụ wireshark hoặc NetworkMiner.

Mục tiêu

- Biết được cách tham gia sân chơi CTF- sân chơi cho dân cybersecurity.
- Hoàn thành bài CTF đầu tiên.

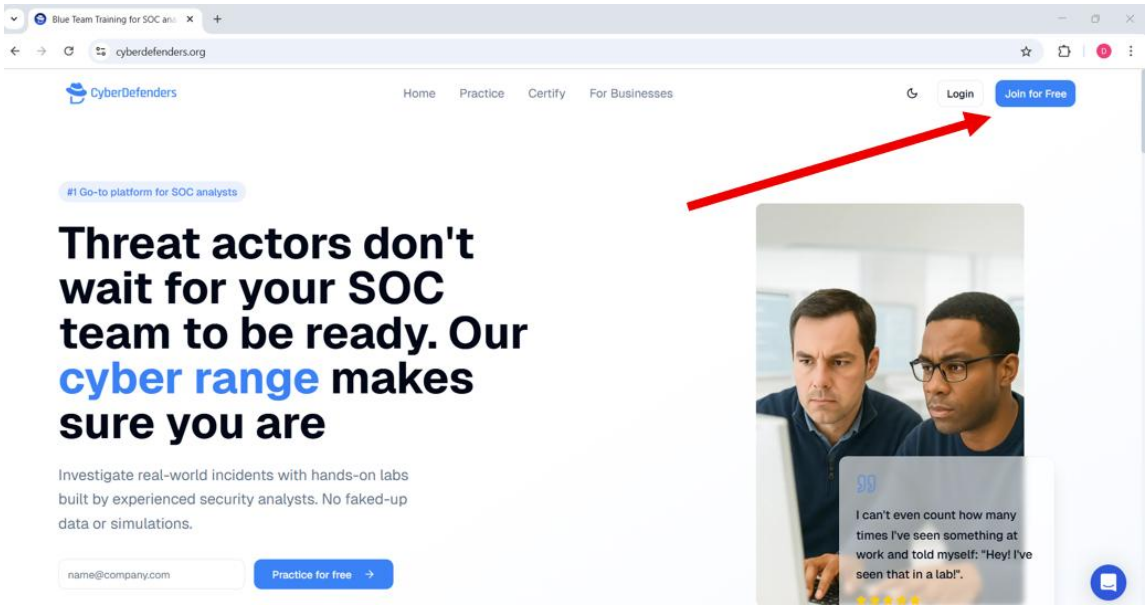
Cảnh báo: Tất cả các bài lab tấn công chỉ được thực hiện trong **môi trường ảo**, **cách ly** và **hợp pháp**. **Tuyệt đối không** áp dụng trên **hệ thống thật** hoặc **mạng không được phép**, mọi vi phạm sẽ bị xử lý theo quy định và pháp luật hiện hành.

Các bài tập thực hành

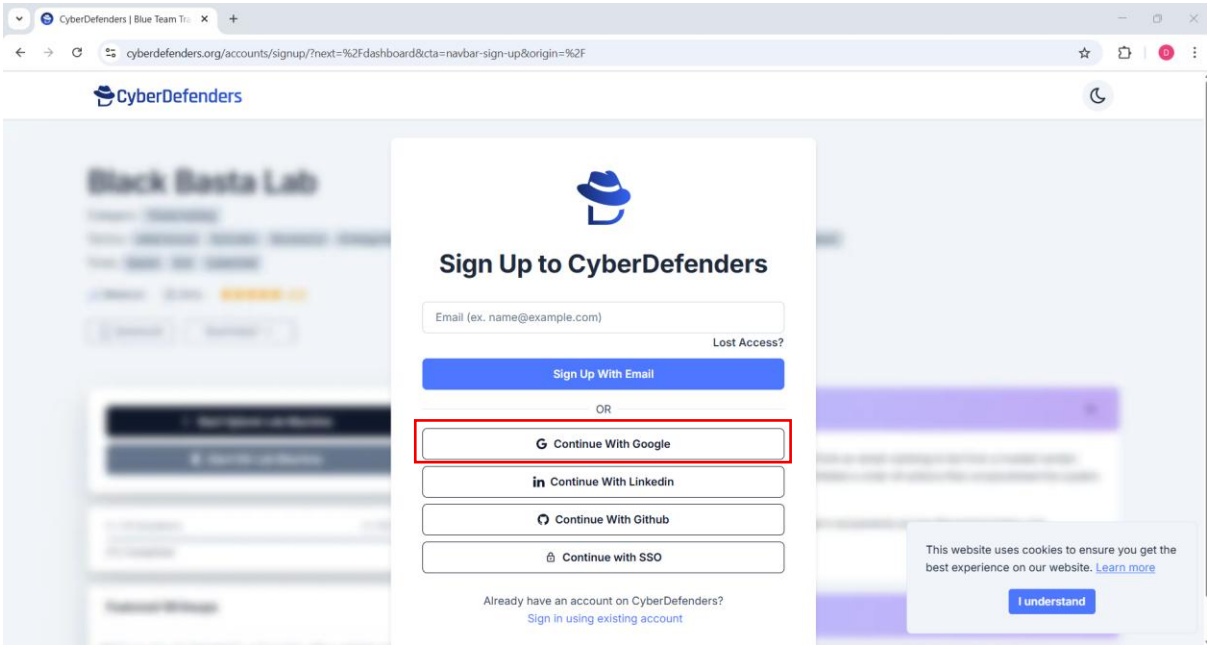
Bài tập 1: Tìm hiểu về trang web CTF cyberdefenders.

Link trang web: Bấm vào đây!! (Nếu không bấm được thì giữ Ctrl để bấm)

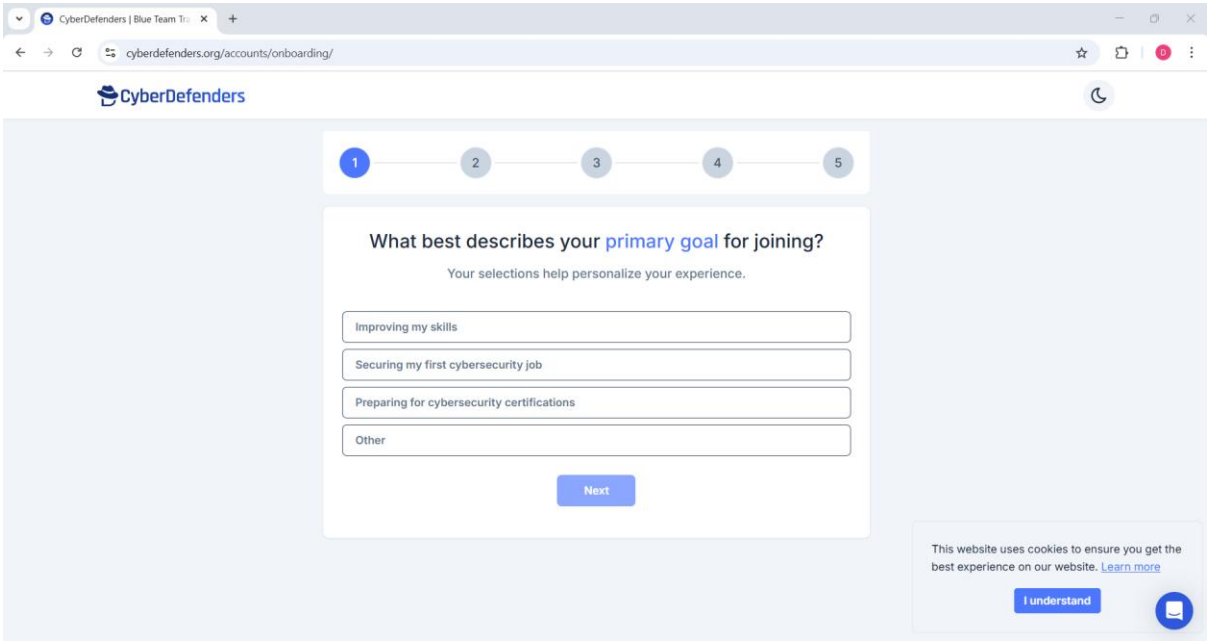
Đây là giao diện của cyberdefenders, nhấn vào Join for Free để đăng kí tài khoản(nếu bạn đã đăng ký tài khoản rồi có thể bỏ qua bước này).



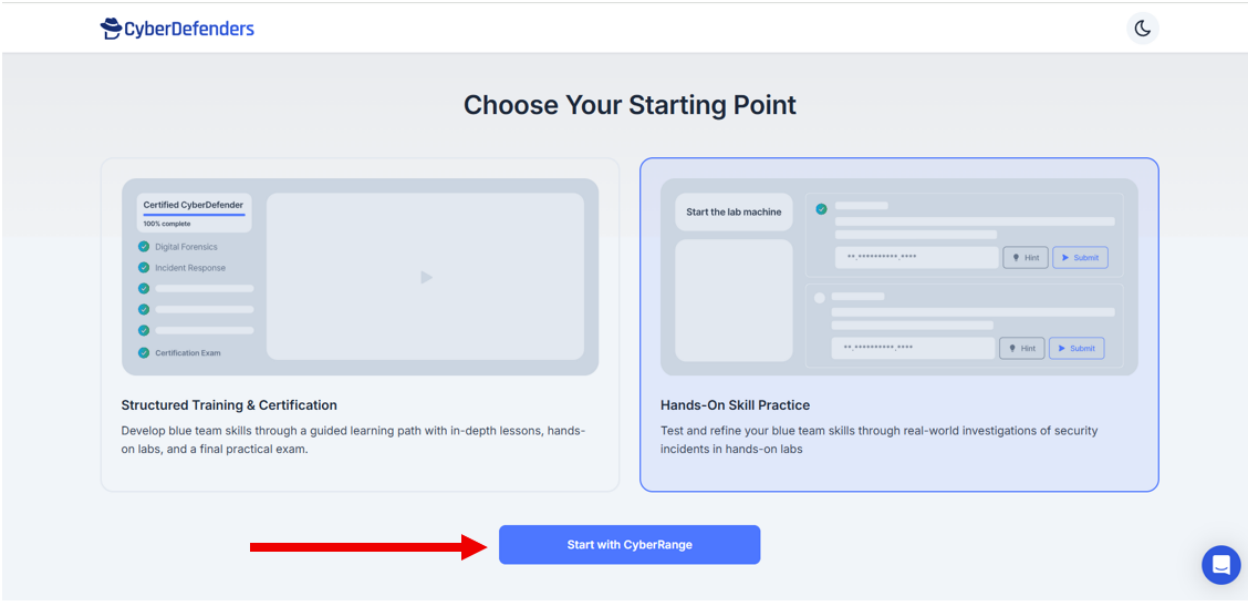
Sau đó sẽ có một cửa sổ hiện lên như hình bên dưới, thực hiện đăng ký tài khoản, chúng ta cũng có thể chọn đăng ký nhanh bằng cách ấn vào Continue With Google.



Sau khi đăng ký xong sẽ có một popup khảo sát bản thân, hoàn thành nhanh rồi ấn next.

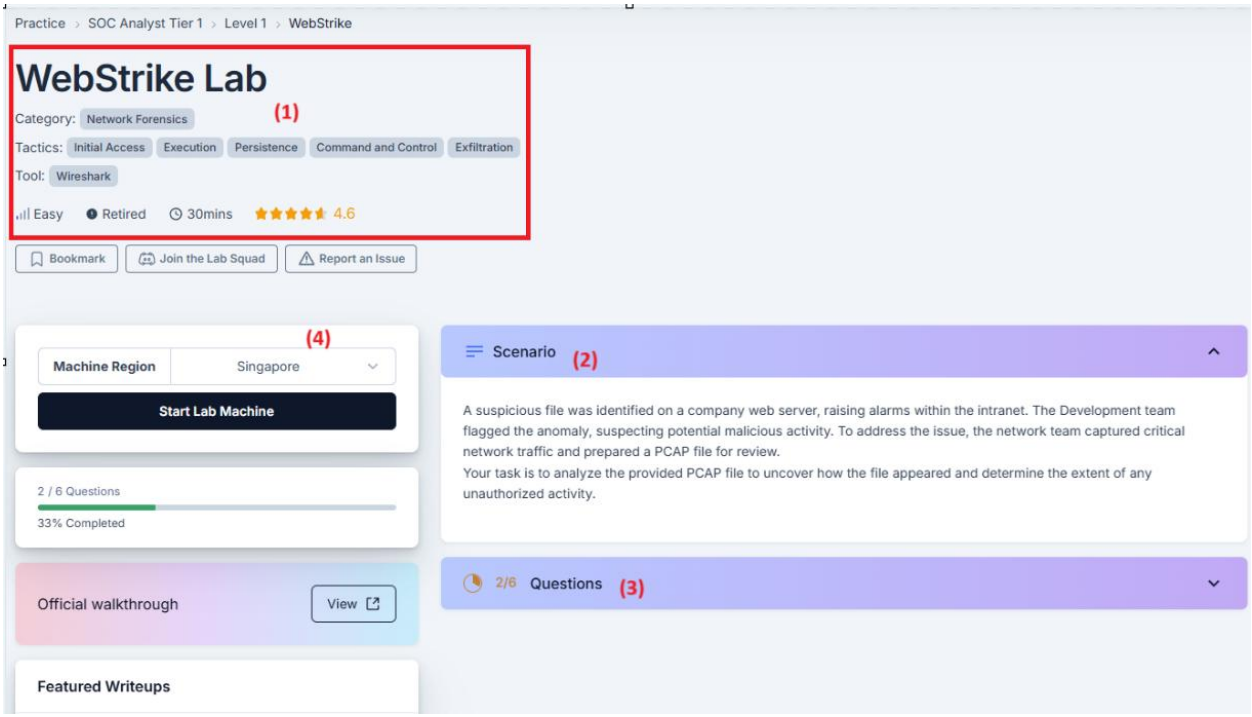


Sau khi hoàn thành khảo sát, chọn vị trí để bắt đầu là Hands-On Skill Pratices, và nhấn Start with CyberRange.

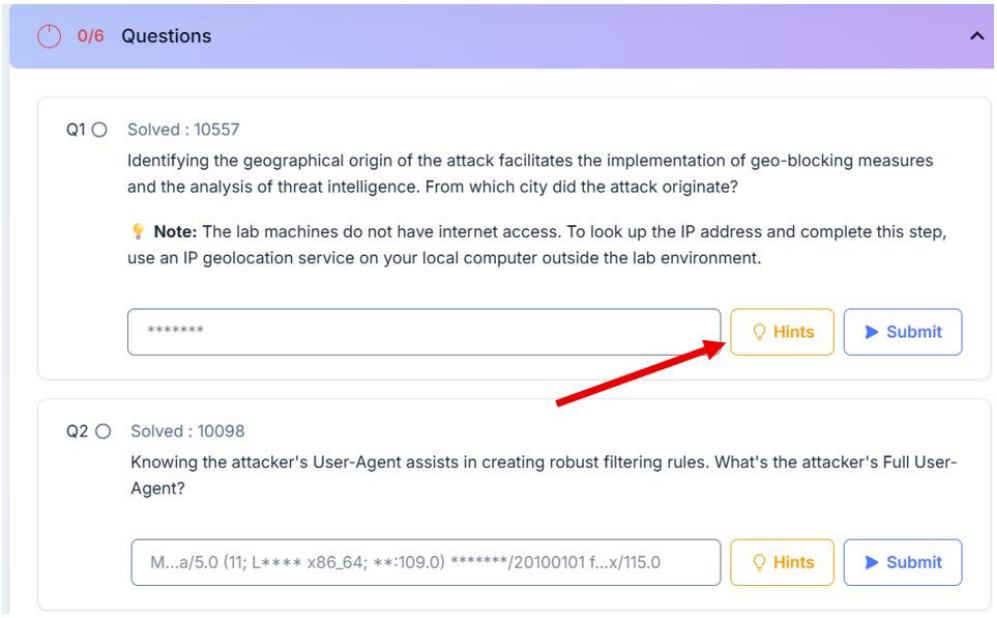


Lúc này bài đầu tiên của bộ môn CTF sẽ hiện lên. Ở đây ta cần lưu ý:

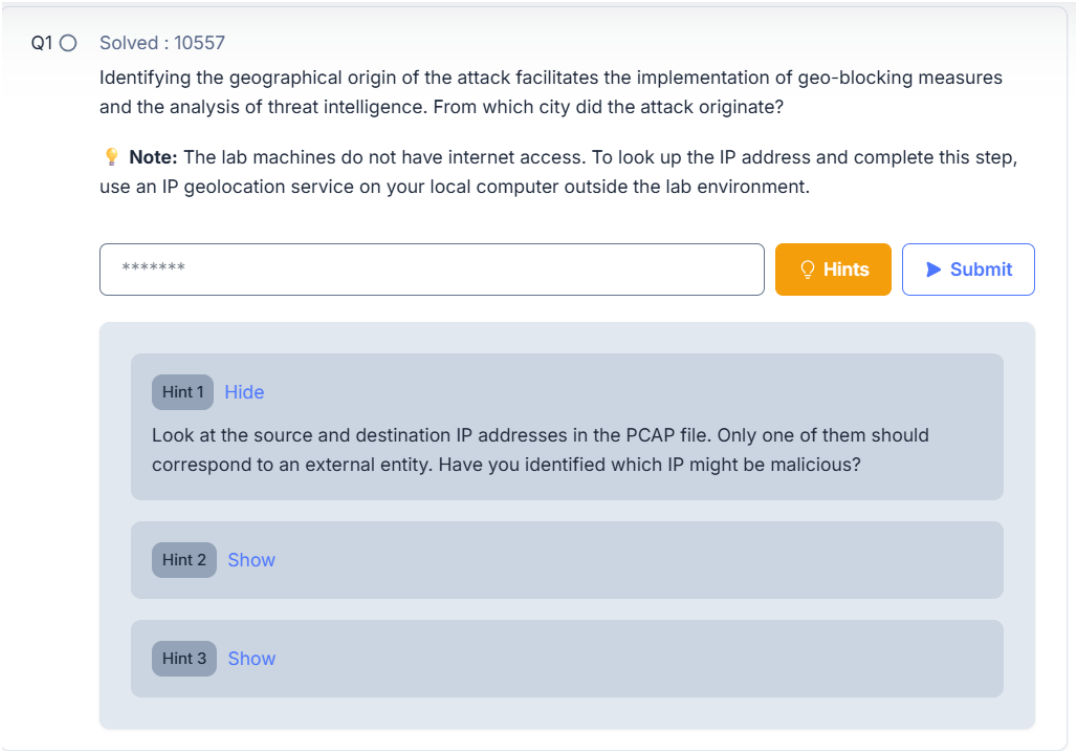
(1) : Ở đây chứa các thuộc tính của bài CTF và tool cần để hoàn thành bài.
(2) : Scenario dùng để mô tả mục tiêu chính của bài CTF này.
(3) : Questions nơi bạn điền đáp án(flags) bạn tìm được để hoàn thành bài.
(4) : Nơi khởi động bài lab để bạn tham gia CTF.



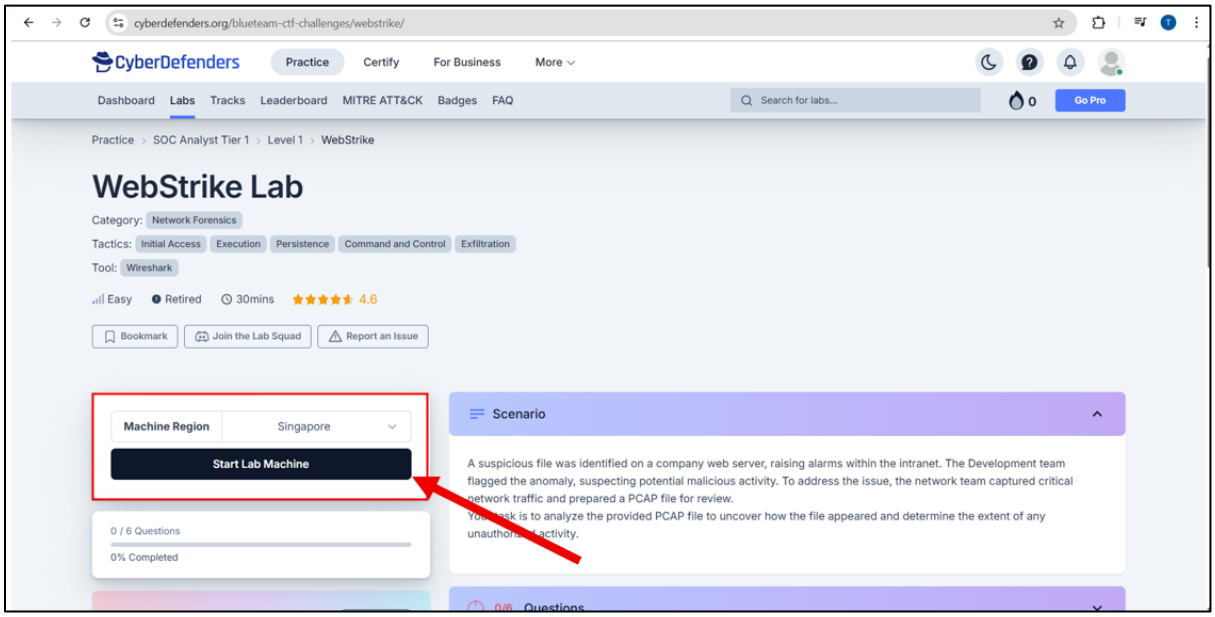
Ở phần questions sẽ có các lá cờ cần bạn đi tìm, thử nhấn vào hint, nó sẽ cho bạn gợi ý để chúng ta đi tìm.



Nhấn vào các Hint bên dưới để xem các gợi ý cho bạn.



Nhấn start lab machine để chờ máy khởi động, và bắt đầu làm bài.

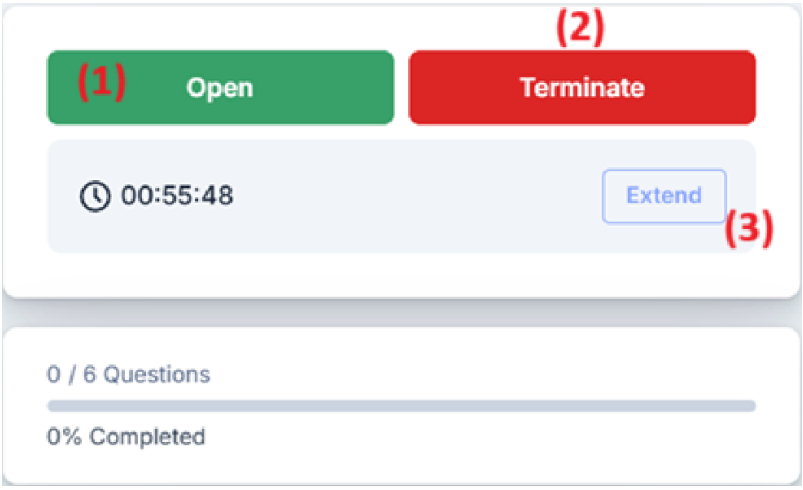


Khi khởi động xong, chúng ta sẽ có:

(1): Open để vào bài lab

(2): Terminate để shut down máy chủ

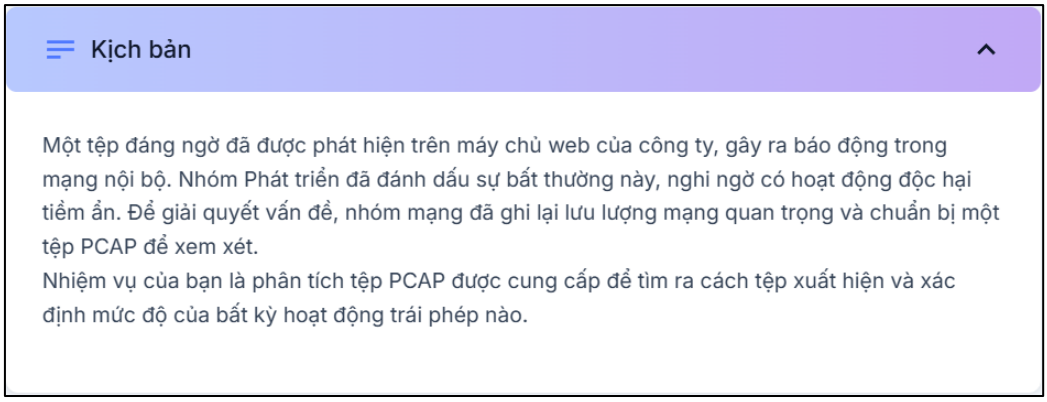
(3): Extend để tăng thêm thời gian máy chủ hoạt động



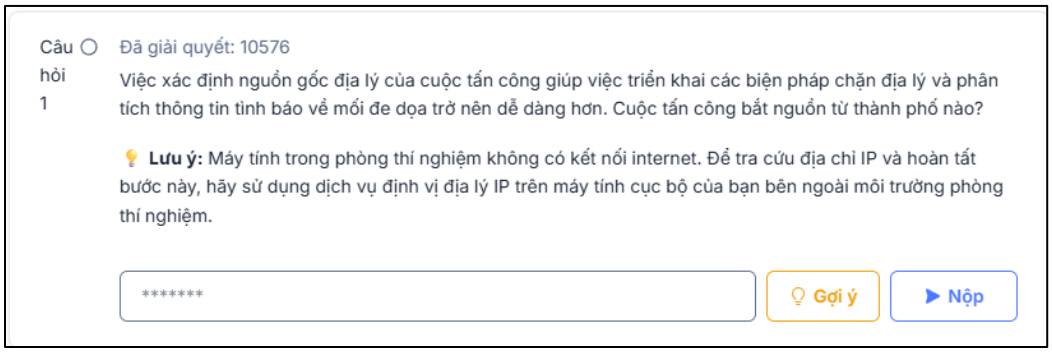
Nhấn Open để vào bài CTF và thực thi bài tập đầu tiên.

Bài tập 2: Tìm lá cờ đầu tiên trong bài CTF.

Đọc qua phần Scenario để chúng ta nắm rõ bối cảnh của bài CTF lần này.

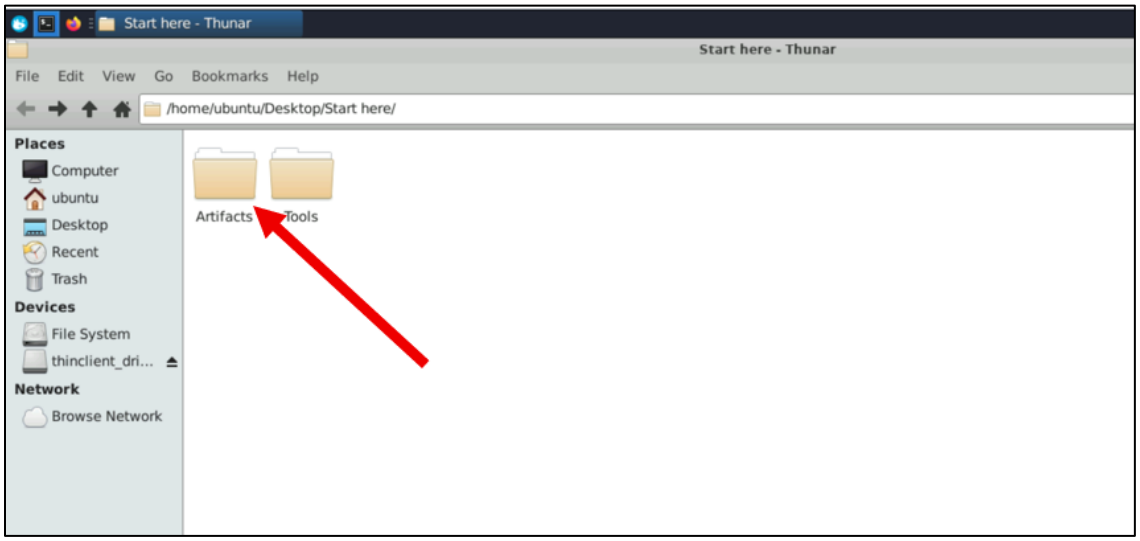


Đọc qua mô tả bên dưới và lưu ý bên dưới để nắm rõ yêu cầu của lá cờ đầu tiên.

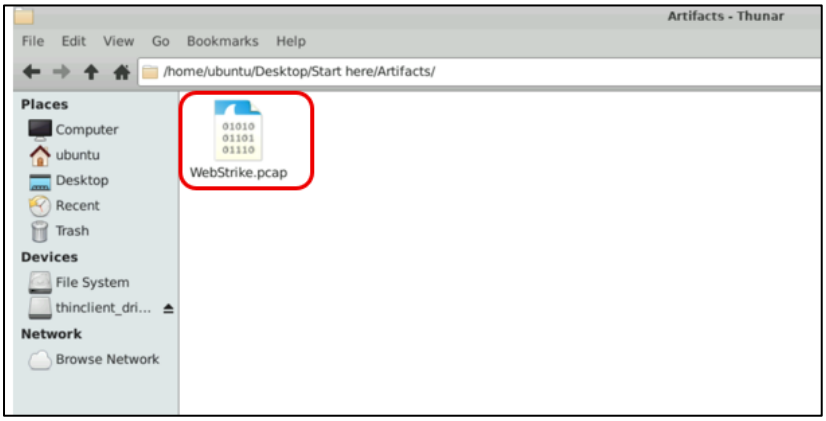


Sau đó qua tab máy chủ đang chạy, nhấn vào thư mục start here.

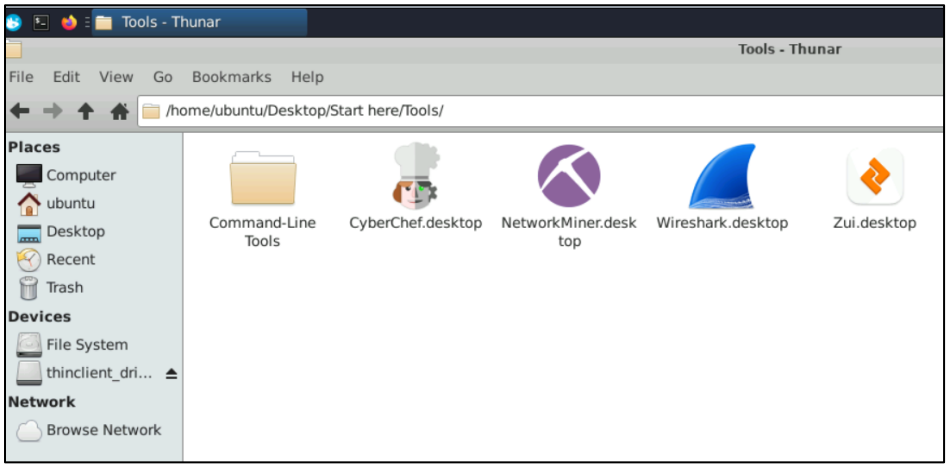
Ở đây có 2 folder, nhấn vào folder artifacts.



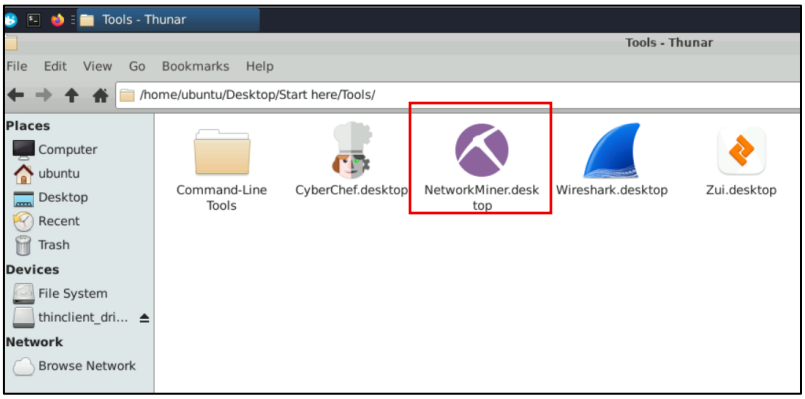
Trong này sẽ có 1 file PCAP được nhắc đến trong kịch bản.



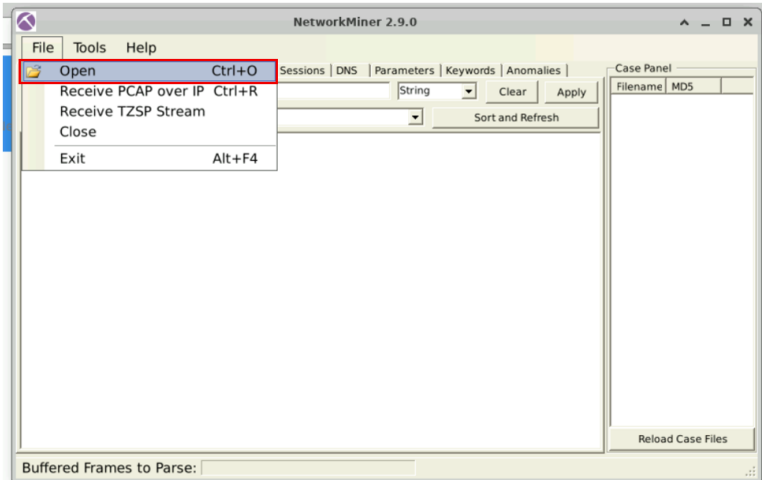
Còn ở phía folder tool, chúng ta sẽ có các tool sau:



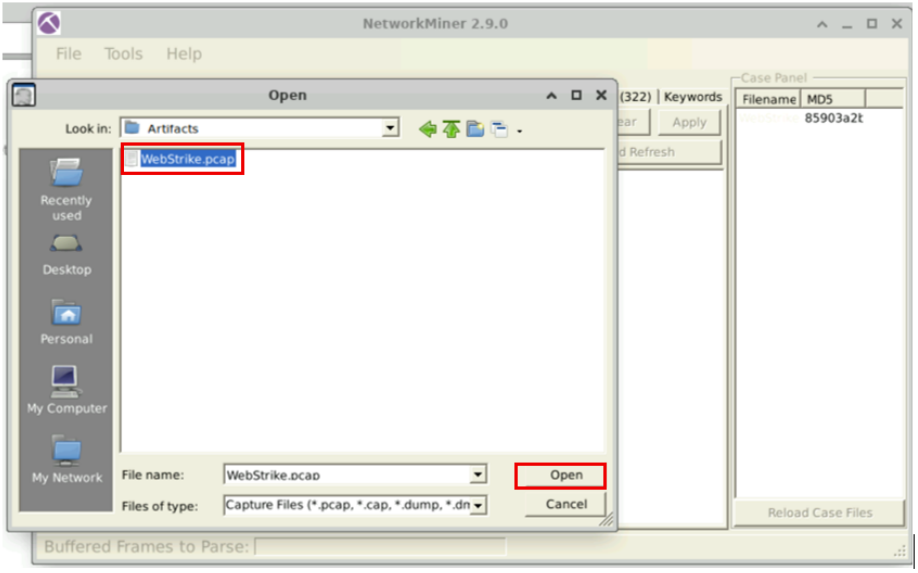
Bạn có thể dùng bất kì tool nào mà bản thân mình hiểu rõ, ở phần hướng dẫn này sẽ sử dụng tool NetworkMiner.desktop



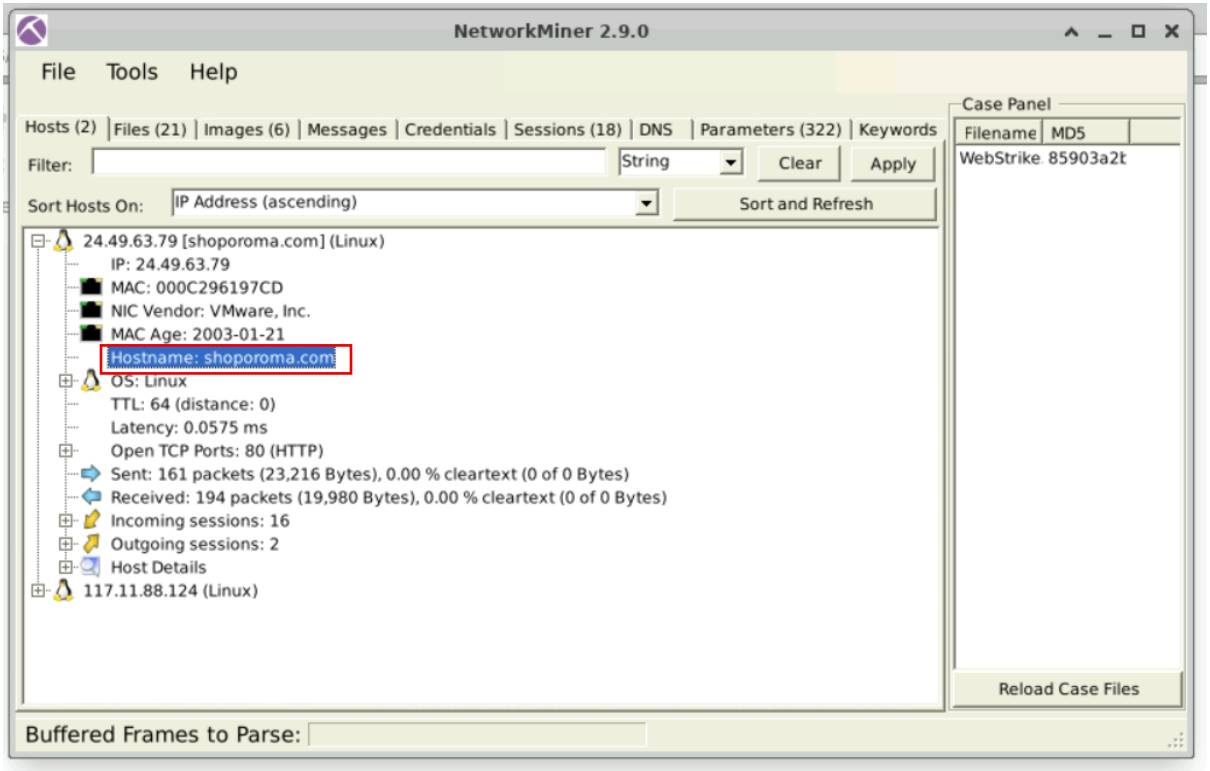
Nhấn vào tool NetworkMiner, sau đó chọn vào File→Open.



Sau đó chọn dẫn tới file PCAP và chọn file PCAP rồi ấn Open

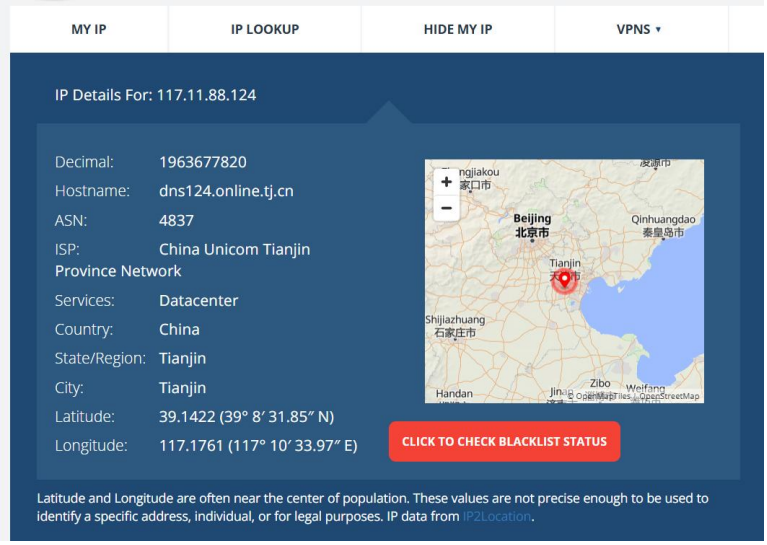


Lúc này các thông tin trong file PCAP sẽ hiện lên, ta có thể thấy trong file này tồn tại 2 host là 24.49.63.79 và 117.11.88.124. Vì 24.49.63.79 là một trang web, nên theo mô tả của bài lab, host còn lại sẽ là attacker.



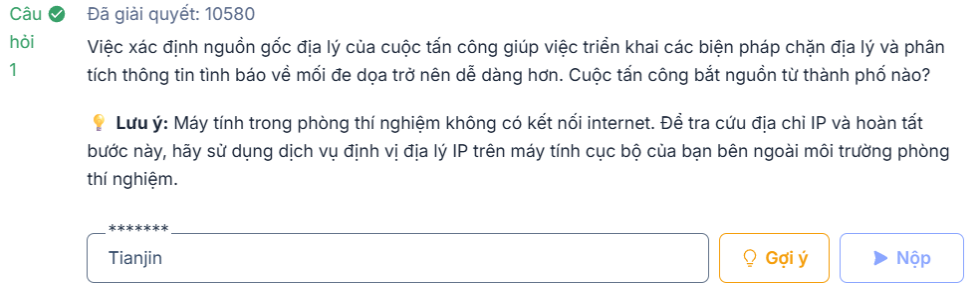
Dựa vào dòng lưu ý, chúng ta dùng bất kì tool IP lookup nào trên google cũng có thể tìm thấy kết quả, ở đây phần hướng dẫn sử dụng tool này(ấn hoặc giữ ctrl để ấn).

Kết quả cho thấy IP này đến từ Trung Quốc Tianjin, vậy Tianjin là đáp án.



Quay lại tab cyberdenders, chúng ta nhập kết quả vào ô flag đầu tiên và nhấn submit.

Như vậy là chúng ta đã tìm được flag đầu tiên của trò chơi CTF

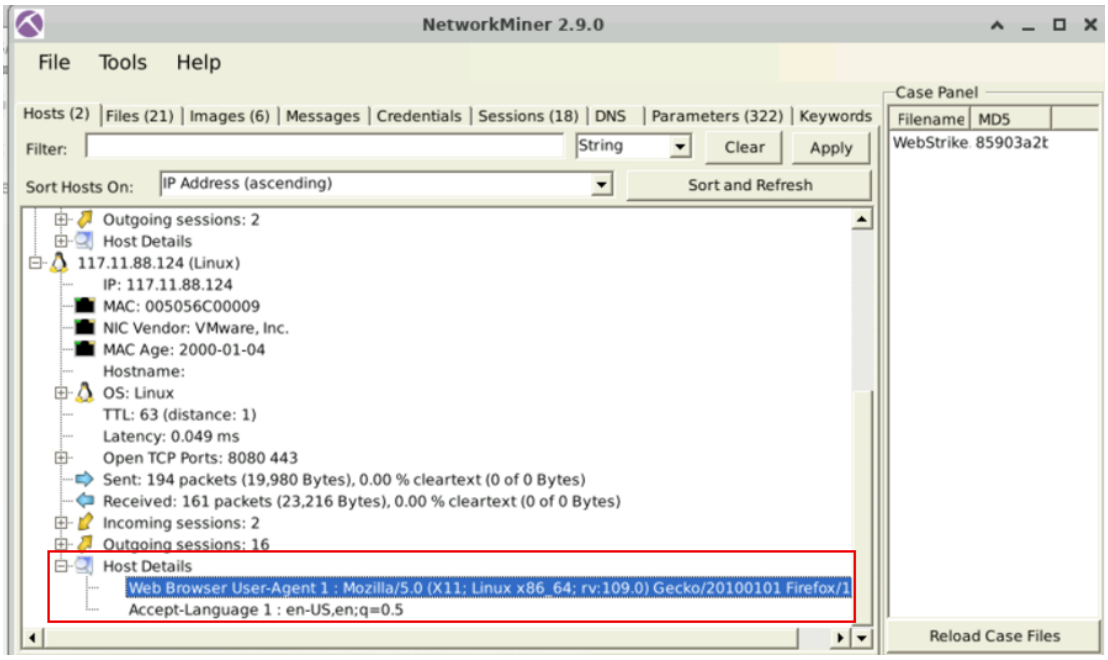


Bài tập 3: Tìm lá cờ thứ hai trong bài CTF.

Đọc qua phần mô tả của lá cờ số 2 để biết thông tin lá cờ cần tìm.

Quay lại tab máy chủ, để tìm được user-agent thực ra là tìm browser dùng để kết nối tới máy chủ, điều này nằm ở Host-detail,

Ấn vào host-detail của host 117.11.88.124 để biết được kết quả.



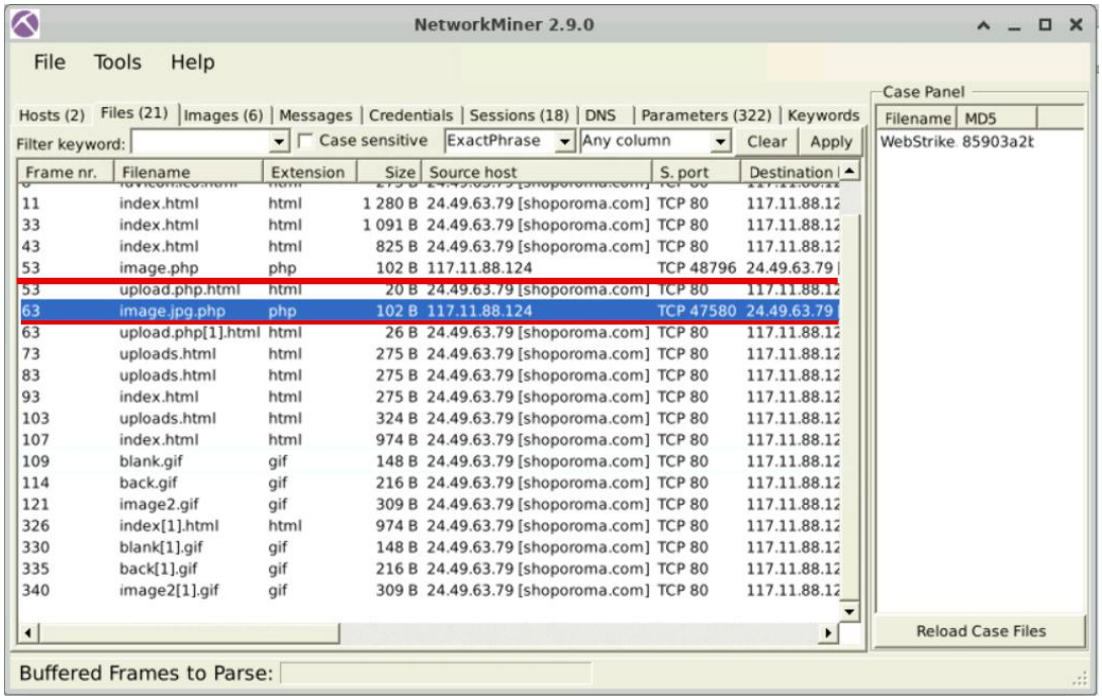
Ấn chuột phải chọn coppy, đó sẽ là phần flag cần tìm, dán kể quả vào phần cờ số 2 và nhấn submit, như vậy ta đã tìm được flag thứ 2.

Bài tập 4: Tìm lá cờ thứ ba trong bài CTF

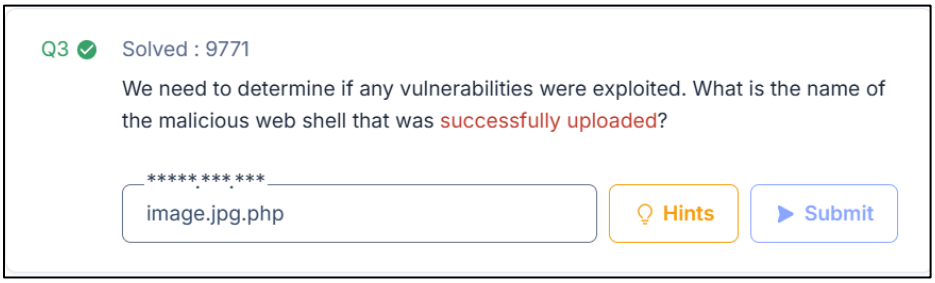
Đọc qua phần yêu cầu của flag thứ 3 bên dưới để nắm được thông tin cần tìm.

Đối với các file tải lên, chúng ta vào file để kiểm tra. Ở đây ta thấy rằng attacker dựa vào filter extension để cố gửi lên một file có chứa mã đọc shell-code, dễ dàng xác định đây là cuộc tấn công RCE.

Sau khi attacker upload file image.jpg.php lên, các file phía sau đều có đuôi file bình thường, vậy đáp án là image.jpg.php

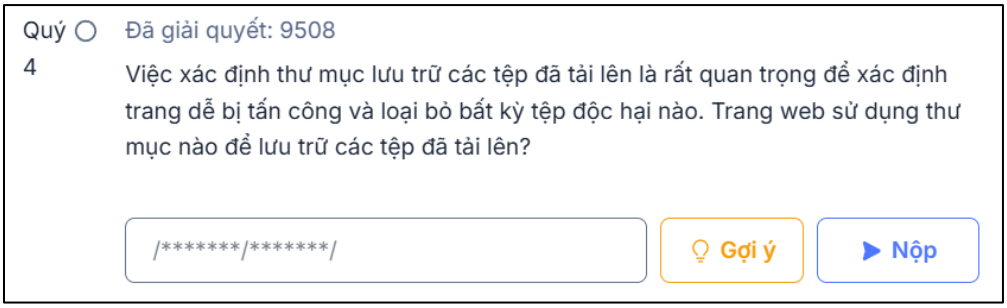


Dán kết quả và ấn submit, như vậy chúng ta đã hoàn thành flag thứ 3.

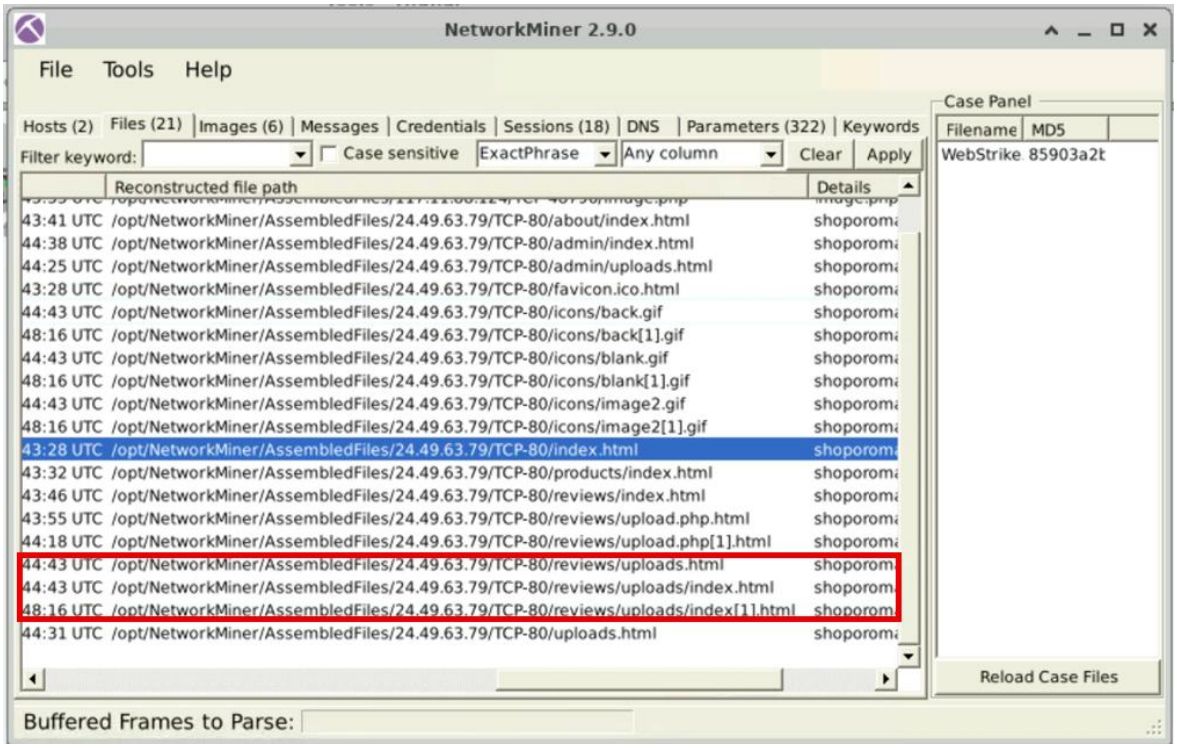


Bài tập 5: Tìm lá cờ thứ tư trong bài CTF.

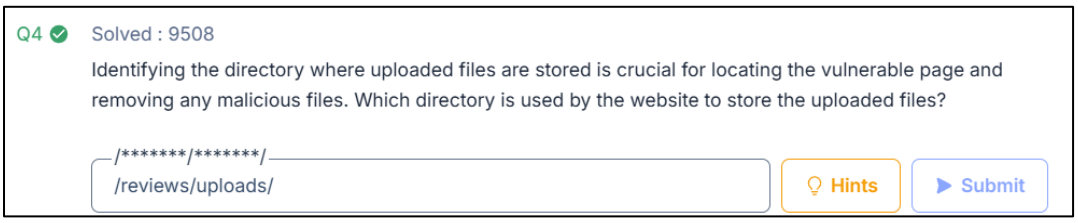
Chúng ta đọc qua mô tả của flag tiếp theo.



Quay lại tab máy chủ, trên NetworkMiner tab File, kéo hết qua bên phải, ta sẽ thấy rằng rằng các file được tải lên theo đường link /reviews/uploads/.

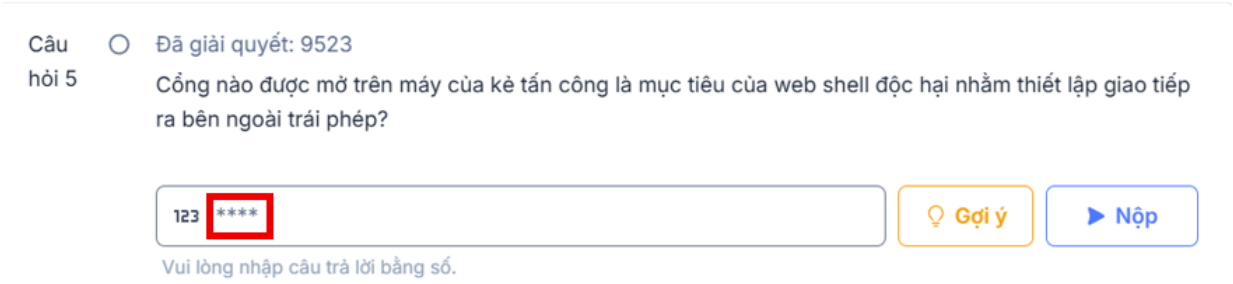


Như vậy kết quả là /reviews/uploads/

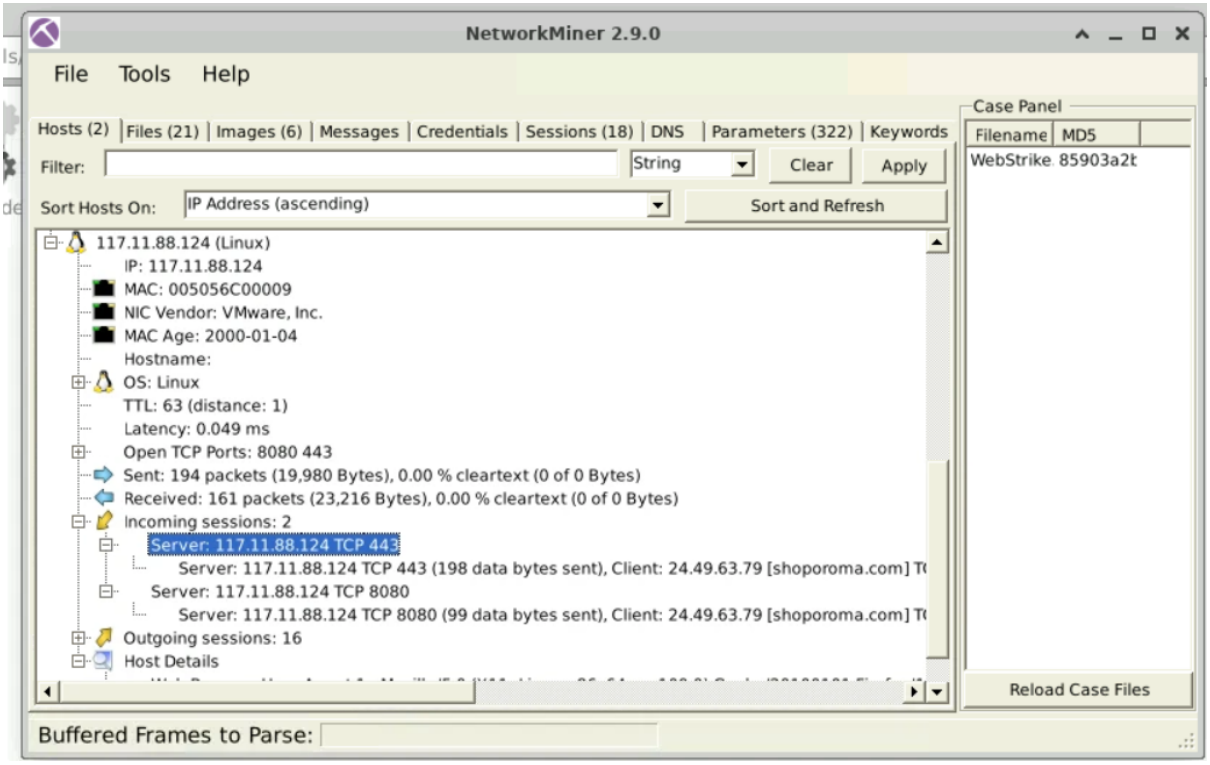


Bài tập 6: Tìm lá cờ thứ năm trong bài CTF.

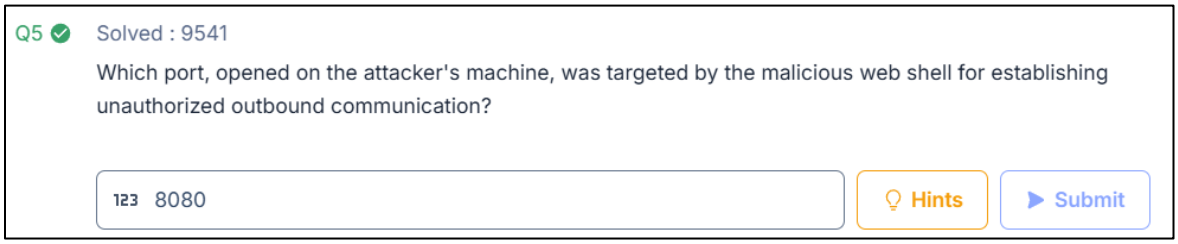
Đọc qua mô tả của cờ thứ 5, đây là lá cờ ta cần tìm là port mở, quan sát kĩ ta thấy đáp án có 4 kí tự.



Truy cập vào Hosts, ta thấy rằng server 117.11.88.124 chỉ mở 2 cổng là 8080 và 443

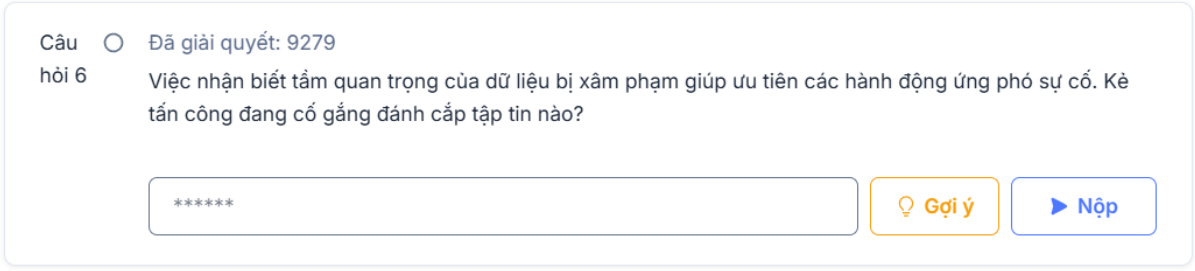


Như vậy đáp án là 8080

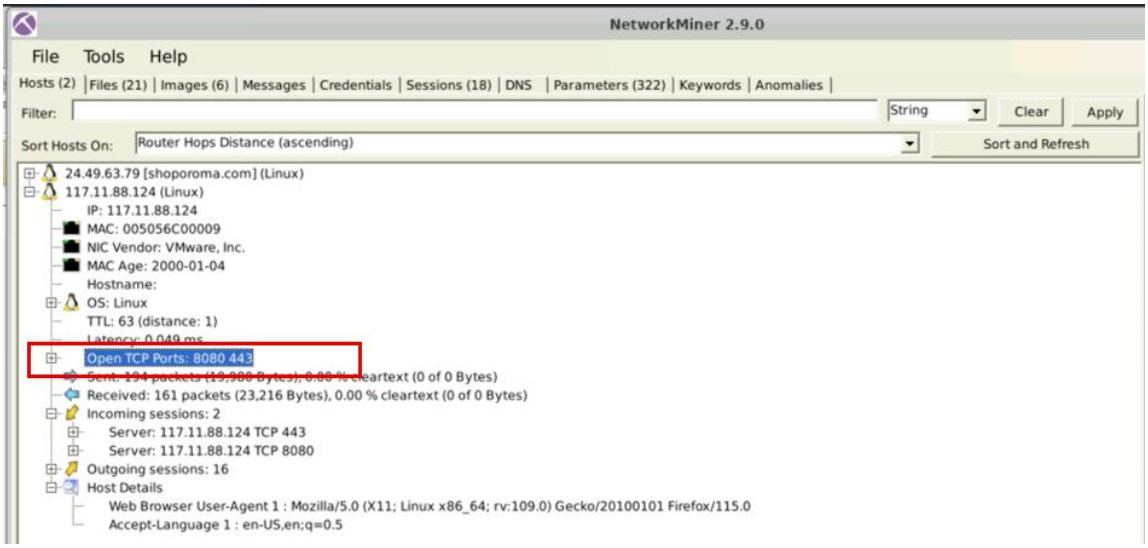


Bài tập 7: Tìm lá cờ cuối cùng trong bài CTF.

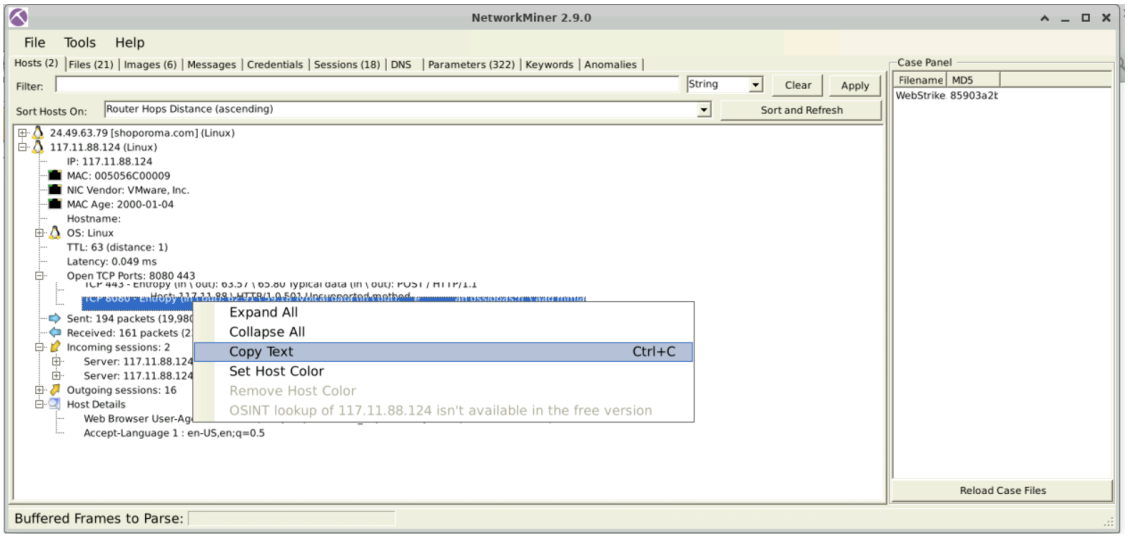
Chúng ta đọc qua mô tả của lá cờ cuối cùng, như vậy chúng ta cần tìm xem attacker đang nhắm tới file gì trong thư mục của mình.



Quay lại tab Host, để điều khiển reverse-shell code, nó sẽ là luồng TCP, và ở cờ số 5 chúng ta cũng biết kẻ tấn công khai thác trên port 8080.



Ấn vào dấu cộng để mở rộng thông tin, sau đó ấn chuột phải vào dòng TCP 8080 và chọn coppy text.



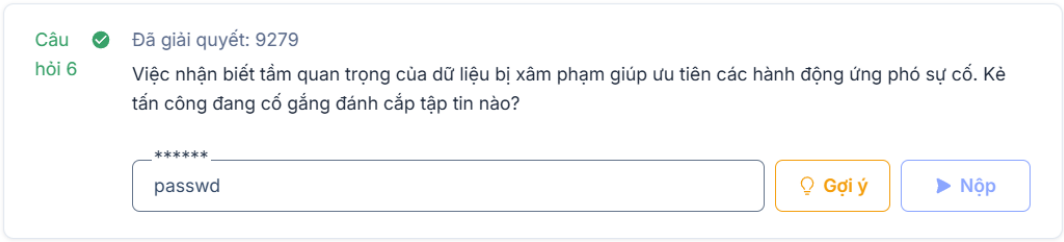
Sau khi coppy, dán ở bất kì đâu, nội dung coppy sẽ nằm ở dưới.

#nội dung coppy

TCP 8080 - Entropy (in \ out): 62.91 \ 59.18 Typical data (in \ out): e an osslooas:n \ aad mmla

aas /d /etc/passwd http

Từ nội dung coppy, chúng ta dễ dàng nhận thấy được kẻ tấn công đang cố gắng khai thác file passwd, đó cũng chính là lá cờ cuối cùng mà chúng ta cần tìm.



⇨ Như vậy chúng ta đã hoàn thành lab CTF đầu tiên ở trang cyberdefenders.