

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.

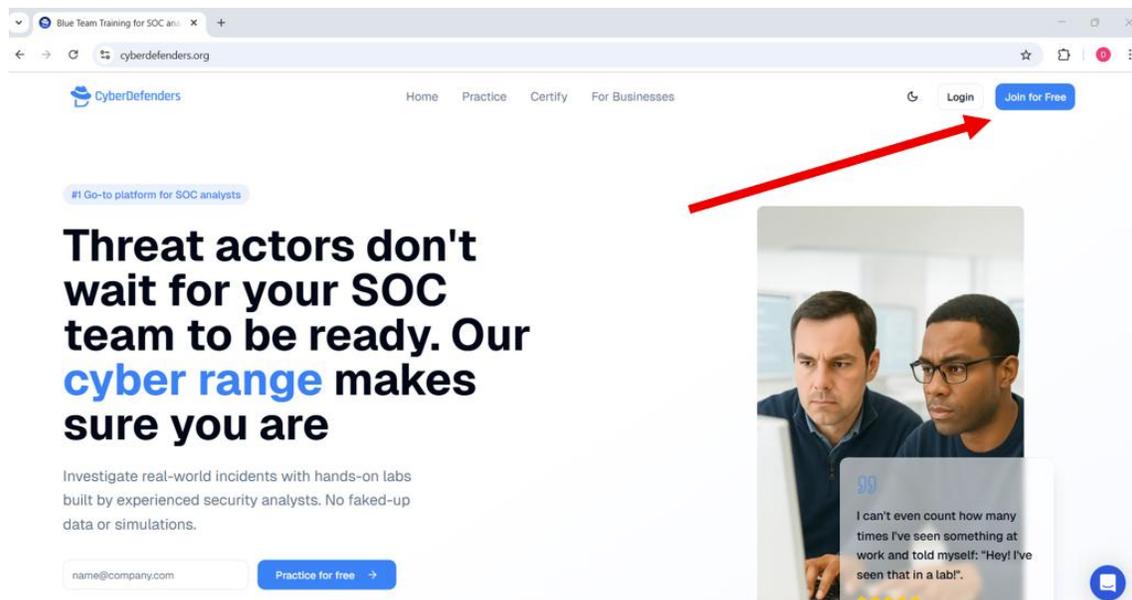
Cảnh báo: Tất cả các bài lab tấn công chỉ được thực hiện trong **môi trường ảo**, cách ly và **hợp pháp**. Tuyệt đối **không** áp dụng trên **hệ thống thật** hoặc **mạng không được phép**, mọi vi phạm sẽ bị xử lý theo quy định và pháp luật hiện hành.

Các bài tập thực hành

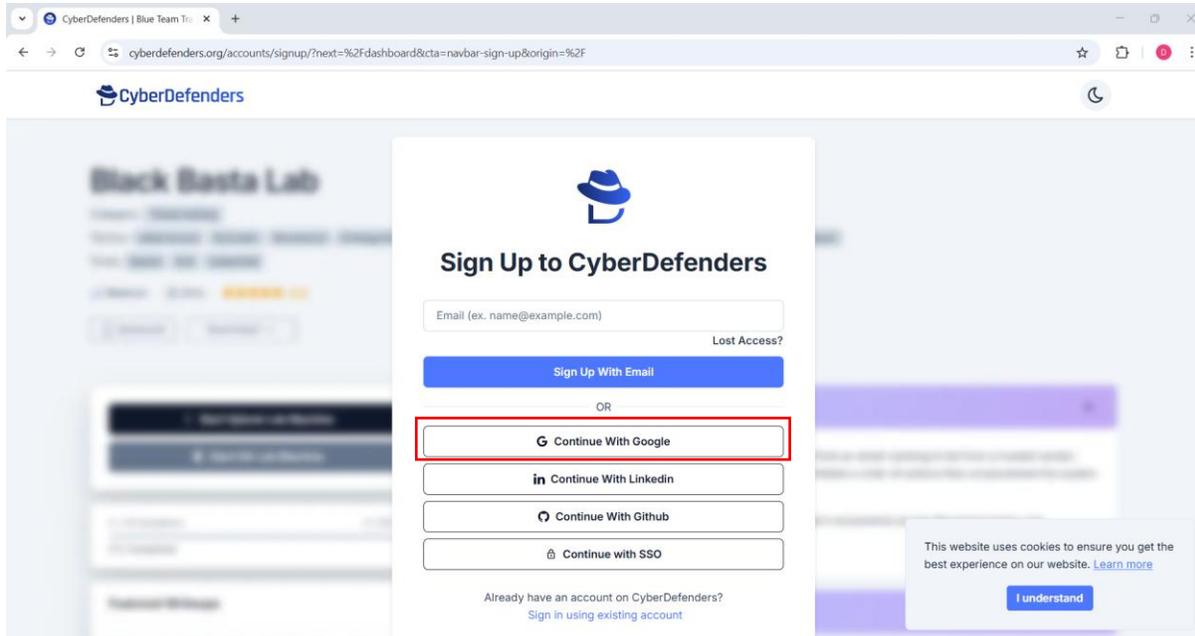
Bài tập 1: Tìm hiểu về trang web CTF cyberdefenders.

Link trang web: [Bấm vào đây!!](https://cyberdefenders.org) (Nếu không bấm được thì giữ Ctrl để bấm)

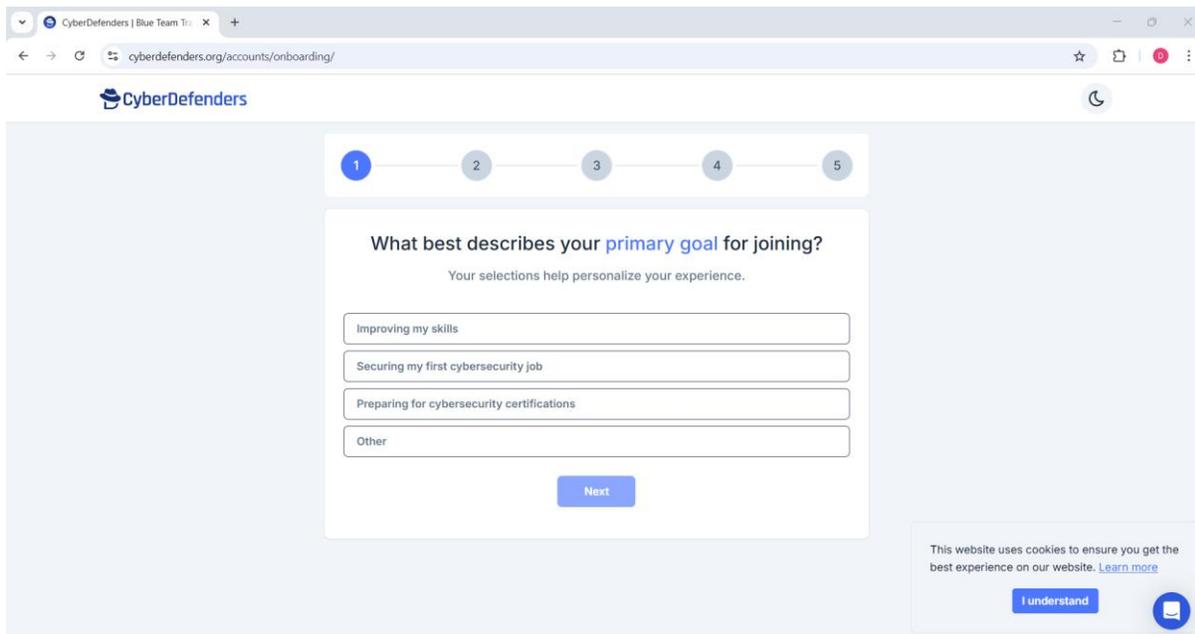
Đây là giao diện của cyberdefenders, nhấn vào Join for Free để đăng kí tài khoản(nếu bạn đã đăng ký tài khoản rồi có thể bỏ qua bước này).



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 Practices, và nhấn Start with CyberRange.

CyberDefenders

Choose Your Starting Point

Certified CyberDefender
100% complete

- Digital Forensics
- Incident Response
-
-
- Certification Exam

Structured Training & Certification
Develop blue team skills through a guided learning path with in-depth lessons, hands-on labs, and a final practical exam.

Start the lab machine

Test and refine your blue team skills through real-world investigations of security incidents in hands-on labs

Hands-On Skill Practice

[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.

Practice > SOC Analyst Tier 1 > Level 1 > WebStrike

WebStrike Lab

Category: Network Forensics (1)

Tactics: Initial Access Execution Persistence Command and Control Exfiltration

Tool: Wireshark

Easy Retired 30mins 4.6

[Bookmark](#) [Join the Lab Squad](#) [Report an Issue](#)

Machine Region: Singapore (4)

[Start Lab Machine](#)

2 / 6 Questions
33% Completed

Official walkthrough [View](#)

Featured Writeups

Scenario (2)

A suspicious file was identified on a company web server, raising alarms within the intranet. The Development team flagged the anomaly, suspecting potential malicious activity. To address the issue, the network team captured critical network traffic and prepared a PCAP file for review.

Your task is to analyze the provided PCAP file to uncover how the file appeared and determine the extent of any unauthorized activity.

2/6 Questions (3)

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.

0/6 Questions

Q1 ○ Solved : 10557
Identifying the geographical origin of the attack facilitates the implementation of geo-blocking measures and the analysis of threat intelligence. From which city did the attack originate?

Note: The lab machines do not have internet access. To look up the IP address and complete this step, use an IP geolocation service on your local computer outside the lab environment.

***** [Hints](#) [Submit](#)

Q2 ○ Solved : 10098
Knowing the attacker's User-Agent assists in creating robust filtering rules. What's the attacker's Full User-Agent?

M...a/5.0 (11; L**** x86_64; **:109.0) *****/20100101 f...x/115.0 [Hints](#) [Submit](#)

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

Q1 ○ Solved : 10557
Identifying the geographical origin of the attack facilitates the implementation of geo-blocking measures and the analysis of threat intelligence. From which city did the attack originate?

Note: The lab machines do not have internet access. To look up the IP address and complete this step, use an IP geolocation service on your local computer outside the lab environment.

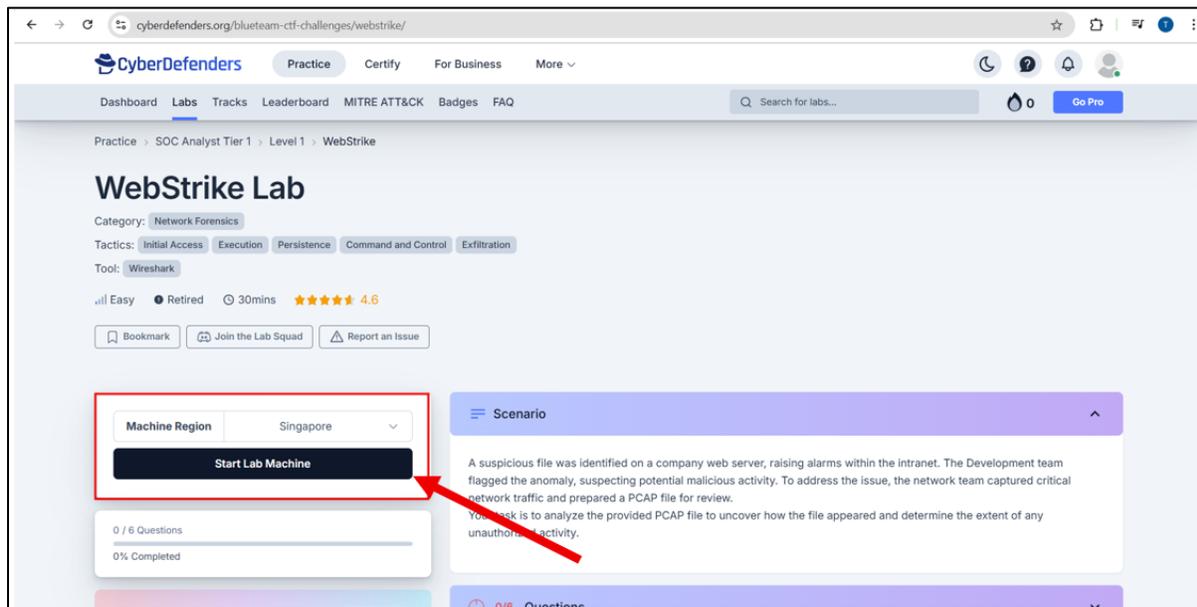
***** [Hints](#) [Submit](#)

Hint 1 [Hide](#)
Look at the source and destination IP addresses in the PCAP file. Only one of them should correspond to an external entity. Have you identified which IP might be malicious?

Hint 2 [Show](#)

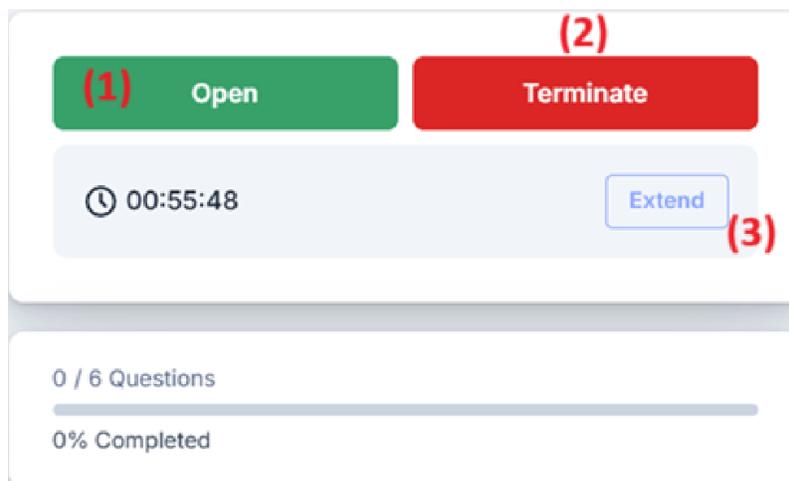
Hint 3 [Show](#)

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.

☰ Kịch bản ^

Một tệp đáng ngờ đã được phát hiện trên máy chủ web của công ty, gây ra báo động trong mạng nội bộ. Nhóm Phát triển đã đánh dấu sự bất thường này, nghi ngờ có hoạt động độc hại tiềm ẩn. Để giải quyết vấn đề, nhóm mạng đã ghi lại lưu lượng mạng quan trọng và chuẩn bị một tệp PCAP để xem xét.

Nhiệm vụ của bạn là phân tích tệp PCAP được cung cấp để tìm ra cách tệp xuất hiện và xác định mức độ của bất kỳ hoạt động trái phép nào.

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

Câu Đã giải quyết: 10576

hỏi

1

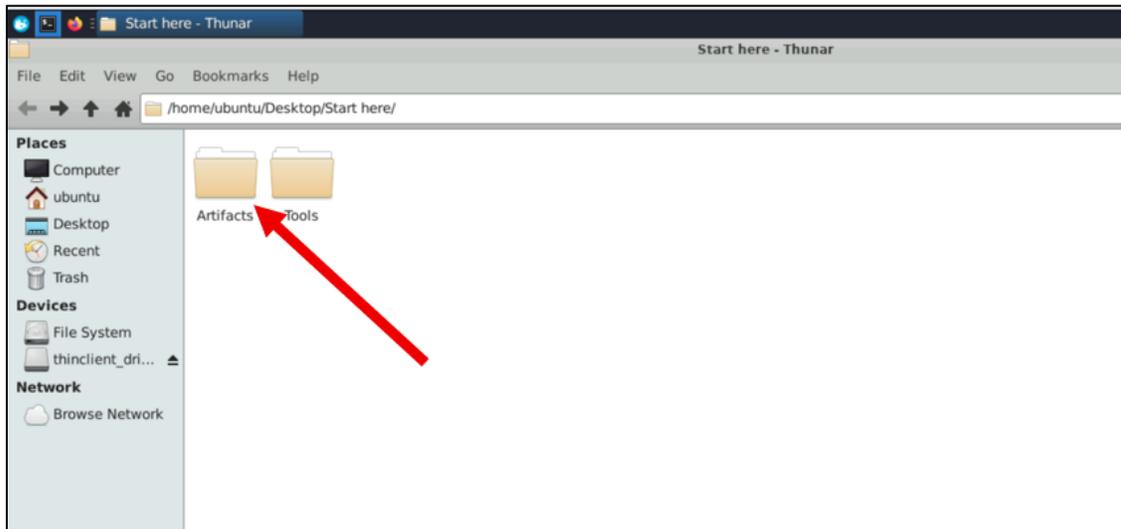
Việc xác định nguồn gốc địa lý của cuộc tấn công giúp việc triển khai các biện pháp chặn địa lý và phân tích thông tin tình báo về mối đe dọa trở nên dễ dàng hơn. Cuộc tấn công bắt nguồn từ thành phố nào?

💡 **Lưu ý:** Máy tính trong phòng thí nghiệm không có kết nối internet. Để tra cứu địa chỉ IP và hoàn tất bước này, hãy sử dụng dịch vụ định vị địa lý IP trên máy tính cục bộ của bạn bên ngoài môi trường phòng thí nghiệm.

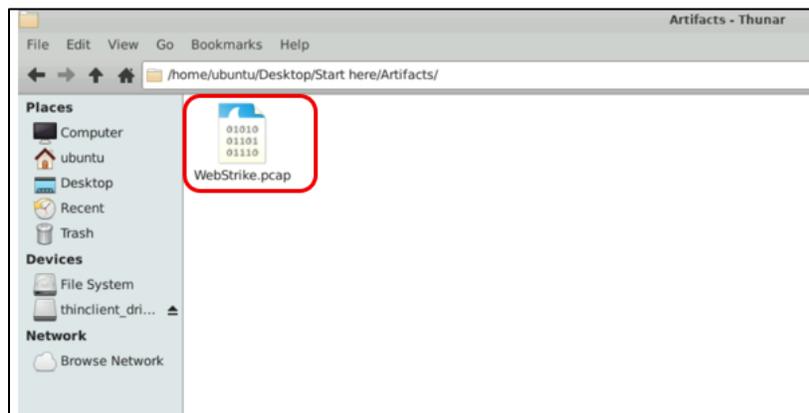
Sau đó qua tab máy chủ đang chạy, nhấn vào thư mục start here.



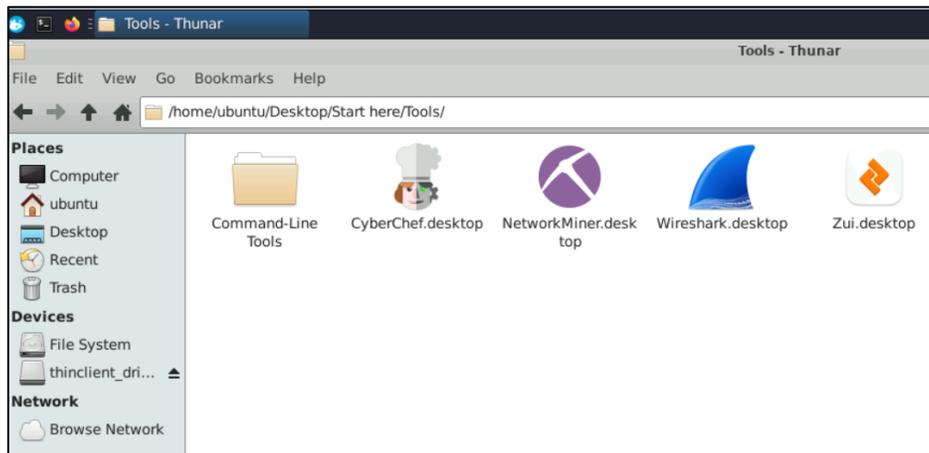
Ở đây có 2 folder, nhấn vào folder artifacts.



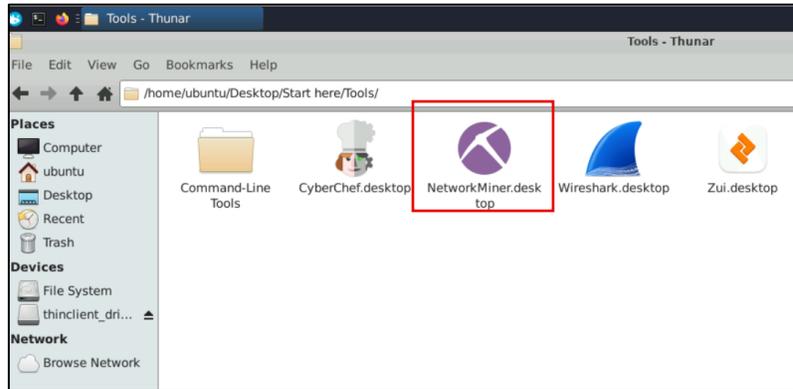
Trong này sẽ có 1 file PCAP được nhắc đến trong kịch bản.



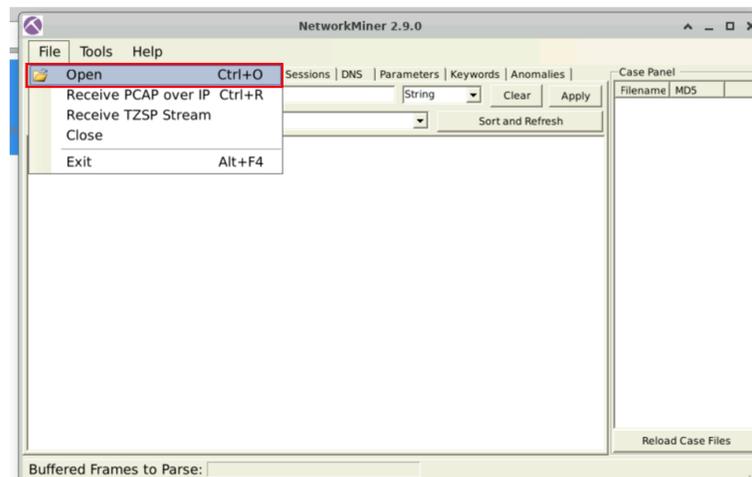
Còn ở phía folder tool, chúng ta sẽ có các tool sau:



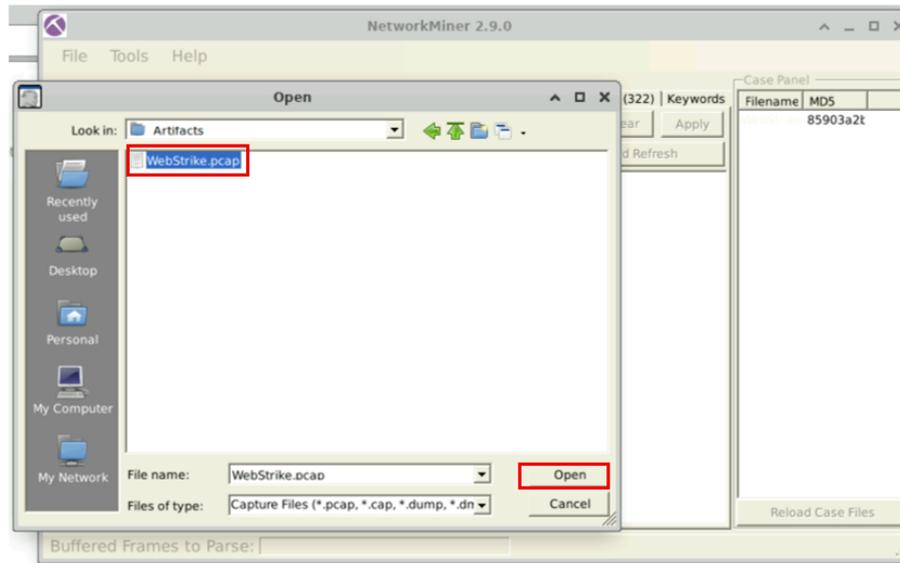
Bạn có thể dùng bất kì tool nào mà bản thân mình hiểu rõ, ở phần hướng dẫn này sẽ sử dụng tool NetworkMiner.desktop



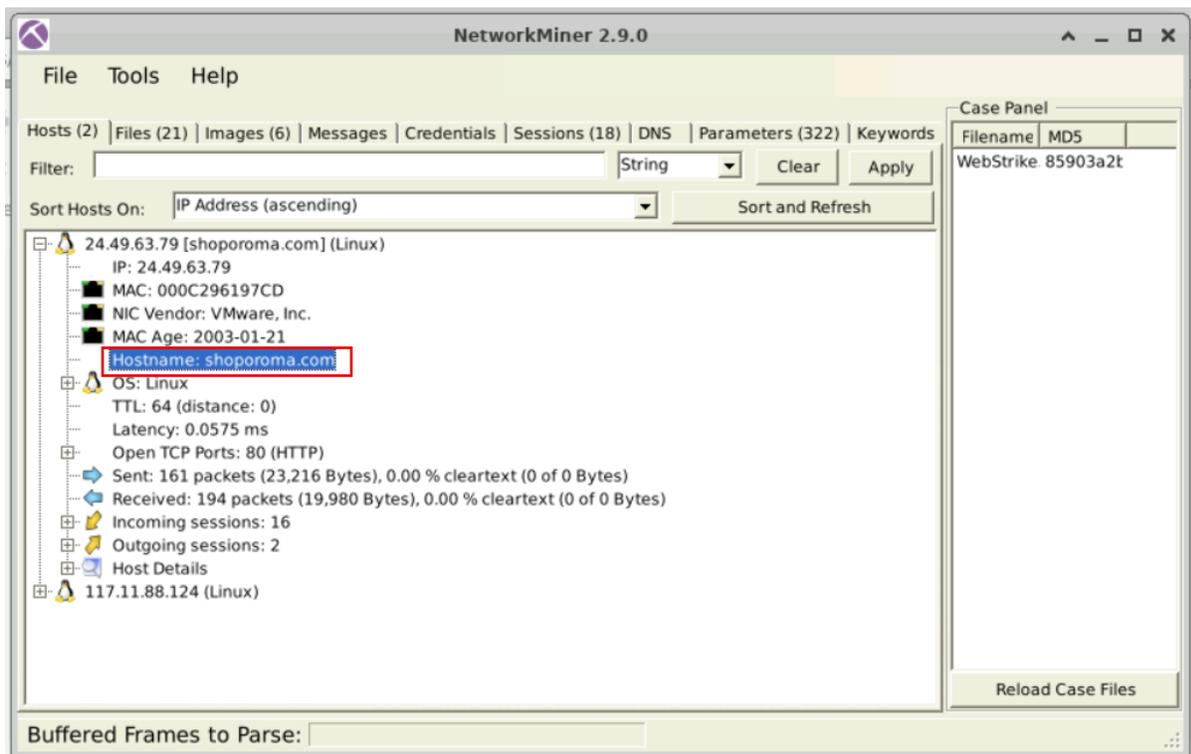
Nhấn vào tool NetworkMiner, sau đó chọn vào File → Open.



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 kỳ 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.

IP Details For: 117.11.88.124

Decimal:	1963677820
Hostname:	dns124.online.tj.cn
ASN:	4837
ISP:	China Unicom Tianjin Province Network
Services:	Datacenter
Country:	China
State/Region:	Tianjin
City:	Tianjin
Latitude:	39.1422 (39° 8' 31.85" N)
Longitude:	117.1761 (117° 10' 33.97" E)

CLICK TO CHECK BLACKLIST STATUS

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address, individual, or for legal purposes. IP data from IP2Location.

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

Câu Đã giải quyết: 10557

hỏi 1

Việc xác định nguồn gốc địa lý của cuộc tấn công giúp việc triển khai các biện pháp chặn địa lý và phân tích thông tin tình báo về mối đe dọa trở nên dễ dàng hơn. Cuộc tấn công bắt nguồn từ thành phố nào?

Lưu ý: Máy tính trong phòng thí nghiệm không có kết nối internet. Để tra cứu địa chỉ IP và hoàn tất bước này, hãy sử dụng dịch vụ định vị địa lý IP trên máy tính cục bộ của bạn bên ngoài môi trường phòng thí nghiệm.

Tianjin

Gợi ý

Nộp

Gợi ý 1 Trốn

Hãy xem địa chỉ IP nguồn và đích trong tệp PCAP. Chỉ một trong hai địa chỉ này tương ứng với một thực thể bên ngoài. Bạn đã xác định được IP nào có thể là độc hại chưa?

Gợi ý 2 Trình diễn

Gợi ý 3 Trình diễn

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

Câu Đã giải quyết: 10580

hỏi 1

Việc xác định nguồn gốc địa lý của cuộc tấn công giúp việc triển khai các biện pháp chặn địa lý và phân tích thông tin tình báo về mối đe dọa trở nên dễ dàng hơn. Cuộc tấn công bắt nguồn từ thành phố nào?

Lưu ý: Máy tính trong phòng thí nghiệm không có kết nối internet. Để tra cứu địa chỉ IP và hoàn tất bước này, hãy sử dụng dịch vụ định vị địa lý IP trên máy tính cục bộ của bạn bên ngoài môi trường phòng thí nghiệm.

Tianjin

Gợi ý

Nộp

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.

Quý Đã giải quyết: 10118

2 Việc biết User-Agent của kẻ tấn công sẽ giúp tạo ra các quy tắc lọc mạnh mẽ. Vậy Full User-Agent của kẻ tấn công là gì?

M...a/5.0 (11; L**** x86_64; **:109.0) **...

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.

NetworkMiner 2.9.0

File Tools Help

Hosts (2) | Files (21) | Images (6) | Messages | Credentials | Sessions (18) | DNS | Parameters (322) | Keywords

Filter: String Clear Apply

Sort Hosts On: IP Address (ascending) Sort and Refresh

Outgoing sessions: 2

Host Details

117.11.88.124 (Linux)

IP: 117.11.88.124

MAC: 005056C00009

NIC Vendor: VMware, Inc.

MAC Age: 2000-01-04

Hostname:

OS: Linux

TTL: 63 (distance: 1)

Latency: 0.049 ms

Open TCP Ports: 8080 443

Sent: 194 packets (19,980 Bytes), 0.00 % cleartext (0 of 0 Bytes)

Received: 161 packets (23,216 Bytes), 0.00 % cleartext (0 of 0 Bytes)

Incoming sessions: 2

Outgoing sessions: 16

Host Details

Web Browser User-Agent 1 : Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

Accept-Language 1 : en-US,en;q=0.5

Case Panel

Filename	MD5
WebStrike	85903a2t

Reload Case Files

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

Quý Đã giải quyết: 10098

2 Việc biết User-Agent của kẻ tấn công sẽ giúp tạo ra các quy tắc lọc mạnh mẽ. Vậy Full User-Agent của kẻ tấn công là gì?

M...a/5.0 (11; L**** x86_64; **:109.0) *****/20100101 f...x/115.0

Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

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

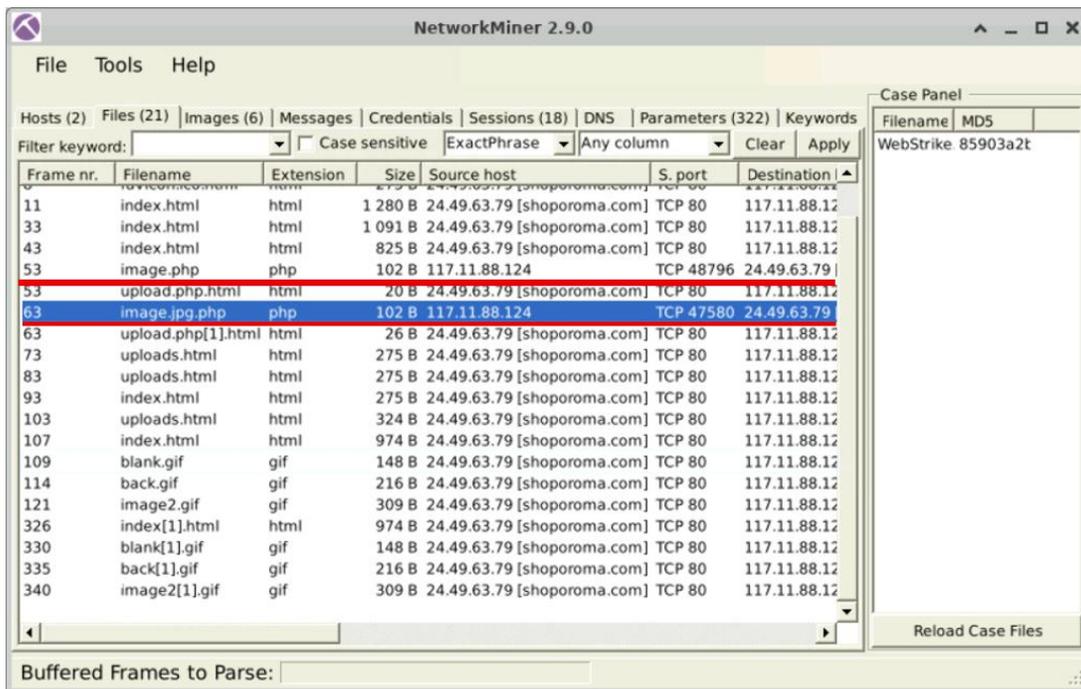
Đọc qua phần yêu cầu của flag thứ 3 bên dưới để nắm được thông tin cần tìm.

Quý Đã giải quyết: 9767

3 Chúng ta cần xác định xem có lỗ hổng nào bị khai thác không. Tên của web shell độc hại đã được **tải lên thành công** là gì ?

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 độc 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



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

Q3 Solved : 9771

We need to determine if any vulnerabilities were exploited. What is the name of the malicious web shell that was **successfully uploaded**?

image.jpg.php

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

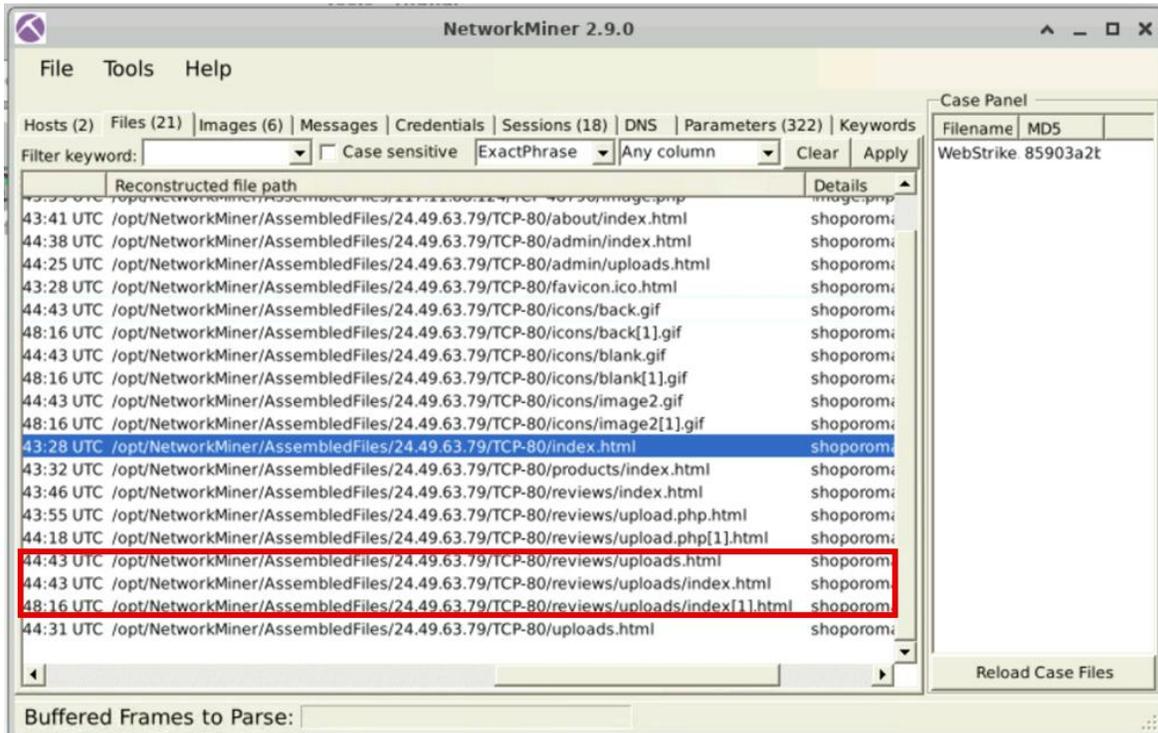
Chúng ta đọc qua mô tả của flag tiếp theo.

Quý ○ Đã giải quyết: 9508

4 Việc xác định thư mục lưu trữ các tệp đã tải lên là rất quan trọng để xác định trang dễ bị tấn công và loại bỏ bất kỳ tệp độc hại nào. Trang web sử dụng thư mục nào để lưu trữ các tệp đã tải lên?

Gợi ý Nộp

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/

Q4 ✓ Solved : 9508

Identifying the directory where uploaded files are stored is crucial for locating the vulnerable page and removing any malicious files. Which directory is used by the website to store the uploaded files?

Hints Submit

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

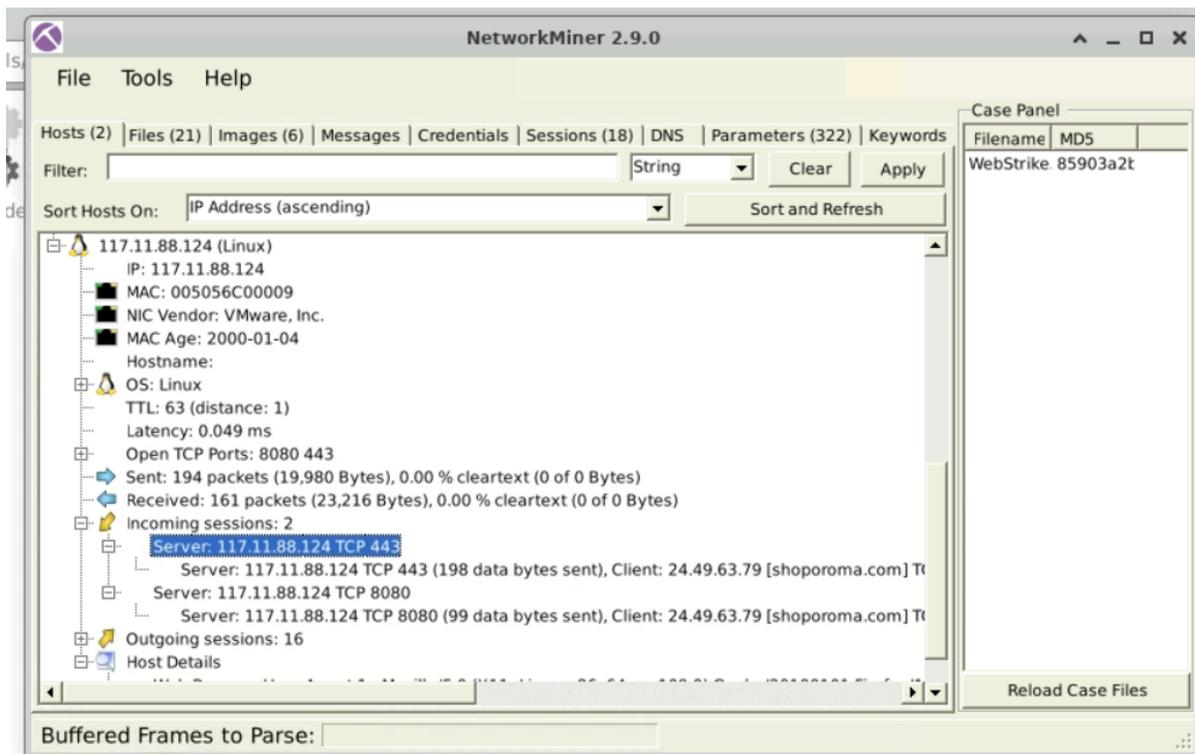
Đọc qua mô tả của cờ thứ 5, đây là lá cờ ta cần tìm là port mở, quan sát kĩ ta thấy đáp án có 4 kí tự.

Câu hỏi 5 Đã giải quyết: 9523

Cổng nào được mở trên máy của kẻ tấn công là mục tiêu của web shell độc hại nhằm thiết lập giao tiếp ra bên ngoài trái phép?

Vui lòng nhập câu trả lời bằng số.

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

Q5 Solved : 9541

Which port, opened on the attacker's machine, was targeted by the malicious web shell for establishing unauthorized outbound communication?

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

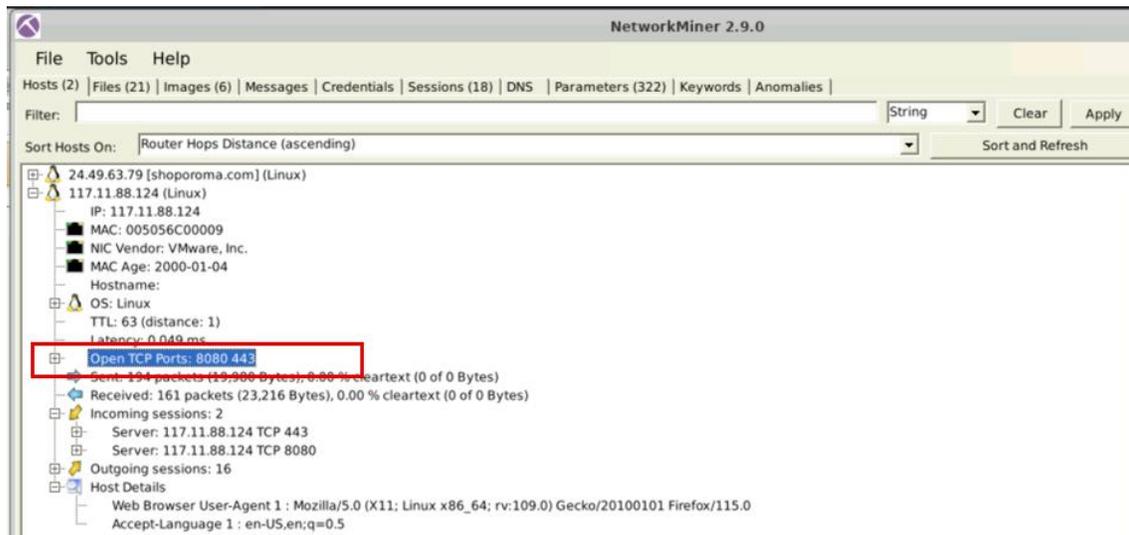
Chúng ta đọc qua mô tả của lá cờ cuối cùng, như vậy chúng ta cần tìm xem attacker đang nhắm tới file gì trong thư mục của mình.

Câu Đã giải quyết: 9279

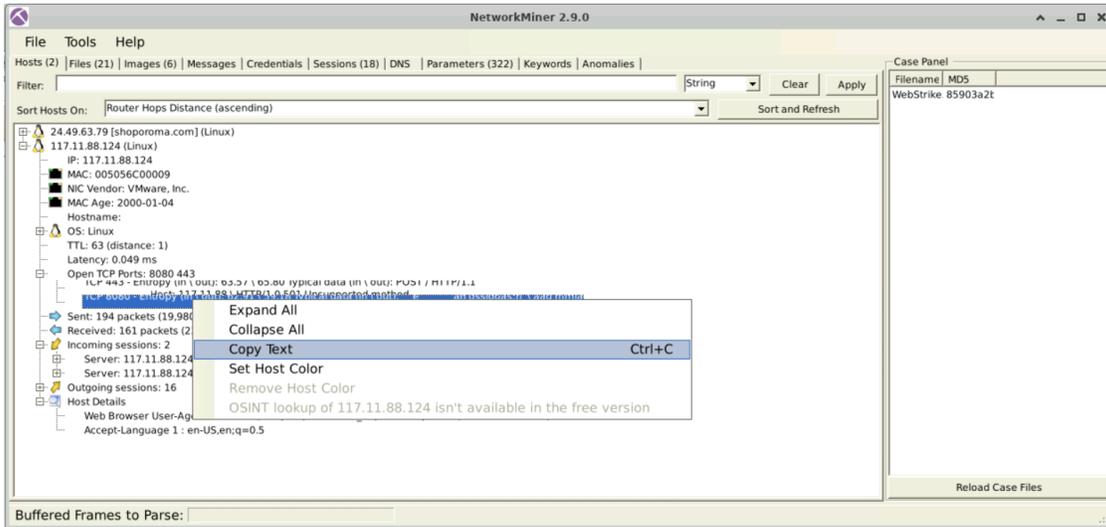
hỏi 6 Việc nhận biết tầm quan trọng của dữ liệu bị xâm phạm giúp ưu tiên các hành động ứng phó sự cố. Kẻ tấn công đang cố gắng đánh cắp tập tin nào?

 Gợi ý  Nộp

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.



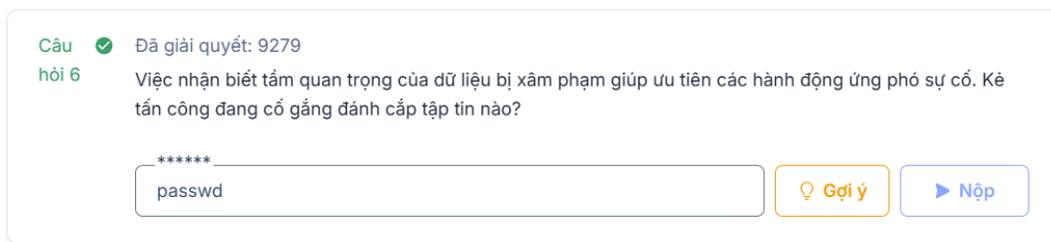
Ấn vào dấu cộng để mở rộng thông tin, sau đó ấn chuột phải vào dòng TCP 8080 và chọn copy text.



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

```
#nội dung copy
TCP 8080 - Entropy (in \ out): 62.91 \ 59.18 Typical data (in \ out):  e      an
osslooa:n \aad mmla
aas /d /etc/passwd http
```

Từ nội dung copy, 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.