**1. Mục đích**

Giúp sinh viên có cơ hội áp dụng các kiến thức phân tích lưu lượng mạng đã học, đồng thời cung cấp kiến thức về một trong các cách tấn công mạng.

**2. Yêu cầu đối với sinh viên**

Có kiến thức cơ bản về phân tích lưu lượng mạng.

**3. Nội dung thực hành**

Chạy lệnh imodule để load bài lab về máy labtainer:

*imodule https://github.com/ptitdseclab/imodule/raw/refs/heads/main/imodule-cyber-attk-mine.tar*

Khởi động bài lab:

*labtainer -r cyber-attk-mine*

*(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)*

Sinh viên tìm kiếm kết quả cho các câu hỏi sau:

**● Task 1: Tìm kiếm thông tin máy nạn nhân**

○ Địa chỉ IP của máy bị tấn công là gì?

- Trong máy có sẵn 2 tệp nhật ký IDS-event của suricata và snort, snort và suricata sẽ hiện lên cảnh báo (alert) khi có những hoạt động mạng bất thường. Tìm kiếm các cảnh báo (alert) trong tệp nhật ký, ta sẽ thấy được các cảnh báo đều đến từ cùng 1 địa chỉ IP

- Vào wireshark bằng cách gõ lệnh:

*wireshark*

- Sử dụng bộ lọc theo IP:

*ip.addr ==****\*ip tìm được\****

○ Tên host của nạn nhân là gì?

*(Gợi ý: tìm trong trường Client Fully Qualified Domain Name)*

○ Địa chỉ MAC của máy nạn nhân là gì?

*Trả lời các câu hỏi bằng cách thu thập các kết quả trả lời như yêu cầu trên, và viết các giá trị vào dòng lệnh, theo thứ tự, trên cùng 1 dòng, đáp án cách nhau 1 dấu cách. Ví dụ:*

*…$ <địa chỉ ip> <tên host> <địa chỉ MAC>*

**● Lý thuyết:**

* **Bộ khai thác lỗ hổng (Exploit Kits - EKs)**được tội phạm mạng sử dụng để lây nhiễm vào máy tính của người dùng khi họ duyệt web mà không hề hay biết. EKs được lưu trữ trên các máy chủ được thiết lập riêng biệt dành cho chúng.
* **Nguyên nhân khiến máy người dùng chuyển hướng đến máy chủ chứa EK:**

+   Điều này thường xảy ra thông qua các trang web bị nhiễm. Kẻ tấn công tấn công vào các trang web hợp pháp, sau đó tiêm các đoạn mã script vào các trang web này. Đoạn mã đó sẽ kết nối máy tính của người dùng đến một máy chủ EK. Tất cả điều này xảy ra không hề có dấu hiệu đáng chú ý khiến cho người dùng hoàn toàn không nhận ra.

+  Chuỗi sự kiện đơn giản nhất có thể được mô tả như sau:

***Trang web hợp pháp bị xâm nhập --> Máy chủ EK***

+   Các tác nhân đe dọa thường sử dụng một máy chủ khác làm cổng chuyển tiếp giữa trang web bị xâm nhập và máy chủ EK.

- Thực tế, các trang web bị nhiễm thường sẽ chuyển hướng lưu lượng người dùng đến các cổng khác:

***Trang web bị xâm nhập --> Cổng chuyển hướng --> EK***

+   Cổng chuyển hướng thường là một trang web khác cũng bị xâm nhập. Ít phổ biến hơn, cổng này là một máy chủ được kẻ tấn công thiết lập riêng. Đôi khi, tội phạm mạng cũng sử dụng **Pastebin**hoặc các công cụ rút gọn URL như **goo.gl**làm cổng chuyển hướng.

- Trong một số trường hợp, có thể có thêm cổng chuyển hướng thứ hai hoặc thứ ba trước khi đến EK:

***Trang web bị xâm nhập --> Cổng thứ nhất --> Cổng thứ hai --> EK***

**● Task 2: Cho biết kẻ tấn công đã sử dụng Angler EK, địa chỉ IP của máy tấn công là 162.216.4.20 hãy trả lời các câu hỏi sau:**

* Thực hiện thêm cột Host để dễ dàng quan sát khi thực hiện:

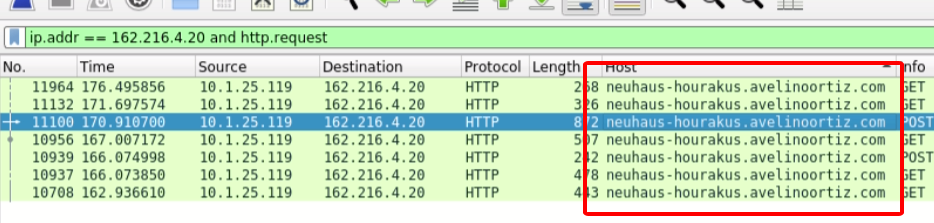
+ Click chuột phải vào tên 1 cột bất kỳ sau đó chọn → Column References → Click dấu + để thêm cột mới

+ Ở cột mới, điều chỉnh Title, Width phù hợp. Đặt Title: Host;  Field: http.host

+ Sau đó có thể xem Host (nếu có) của gói tin trên giao diện chính của wireshark

* Lọc theo http.request và địa chỉ IP như dưới đây sẽ thấy được các đường link dẫn đến Angler EK:

*ip.addr == 162.216.4.20 and http.request*



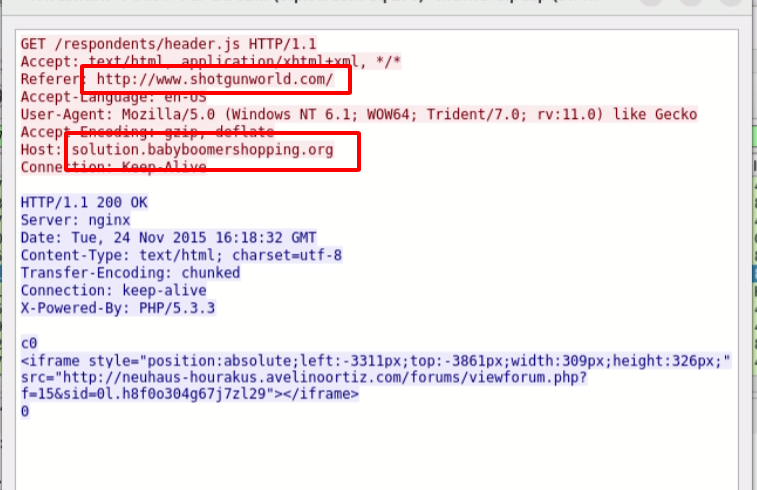
* Để kiểm tra xem máy tính của nạn nhân truy cập đến các đường link này như thế nào, lọc những gói tin ip có chứa tên host với lệnh trên thanh địa chỉ:

*ip contains "****tên host tìm được****”*

* Sau khi lọc, ta sẽ chú ý đến gói tin đầu tiên, khi dữ liệu chuyển hướng.

Chuột phải → Follow → TCP Stream

* Khi đó ta có thể thấy được trang web trước đó ở dòng Referer và đường link dẫn tới trang web được nhúng trong iframe.



* Tiếp tục tìm theo máy chủ (Host) mới tìm được.

*ip contains "****tên host tìm được****”*

* Tiếp tục kiểm tra gói tin đầu tiên (Khi dữ liệu chuyển hướng):

Chuột phải → Follow → TCP Stream

* Có thể nhận thấy trang link chuyển hướng cũng được nhúng trong iframe của trang web. Ở đây ta có thể xác định thời gian máy nạn nhân bị tấn công. Trả lời các câu hỏi sau:

○ Trong cuộc tấn công này có bao nhiêu cổng chuyển hướng (Không tính trang web bị nhiễm)?

○ Host của trang web bị nhiễm là gì?

○ Tìm thời gian máy bắt đầu bị nhiễm mã độc *(DD/MM/YYYY hh:mm:ss)*

*Trả lời các câu hỏi theo thứ tự, trên cùng 1 dòng, đáp án cách nhau 1 dấu cách.*

**● Trả lời câu hỏi:**

* Sinh viên tạo 1 file và lưu kết quả vào các dòng khác nhau với định dạng:

Task *x:*(*Kết quả*)

* Lệnh tạo file:

*nano tên\_file*

- Thực hiện biên dịch chương trình result.c và chạy:

*gcc result.c -o result*

*./result*

-     Sau khi chạy chương trình, nhập tên file chứa đáp án vào để kiểm tra kết quả.

**● Kết thúc bài lab:**

*stoplab*

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Kiểm tra kết quả:

*checkwork*