-

Bài thực hành: Tìm hiểu về công cụ Wireshark

**TÌM HIỂU BÀI THỰC HÀNH**

**ptit-network-tracing**

**Giảng viên:** Đinh Trường Duy

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

* + 1. Nội dung và hướng dẫn bài thực hành
  1. Mục đích

Wireshark là một công cụ phân tích gói tin mạng mã nguồn mở và miễn phí. Nó được sử dụng rộng rãi trong lĩnh vực mạng máy tính để ghi lại và phân tích các gói tin mạng đi qua một mạng hoặc một giao diện mạng cụ thể trên máy tính. Wireshark cho phép người dùng xem và phân tích dữ liệu mạng theo nhiều cách khác nhau, bao gồm xem các gói tin cá nhân, thống kê dữ liệu mạng, và phân tích các giao thức mạng khác nhau.

Công cụ này được cung cấp trên nhiều nền tảng hệ điều hành khác nhau, bao gồm Windows, macOS và Linux, làm cho nó trở thành một trong những công cụ phân tích gói tin mạng phổ biến nhất trên thị trường. Wireshark cung cấp một giao diện người dùng dễ sử dụng và linh hoạt, cho phép người dùng tìm hiểu và khám phá các hoạt động mạng một cách chi tiết.

Sử dụng Wireshark để truy vết mã độc sẽ giúp sinh viên hiểu về cách sử dụng công cụ Wireshark để phân tích gói tin mạng và xác định các hoạt động độc hại trên mạng.

* 1. Yêu cầu đối với sinh viên

Sinh viên cần có kiến thức cơ bản về hệ điều hành Linux và các khái niệm cơ bản về phân tích malware để hiểu và áp dụng công cụ Wireshark. Hiểu biết về các công cụ như VirusTotal có thể hữu ích để bổ sung kiến thức trong quá trình sử dụng Wireshark.

* 1. Nội dung thực hành

Trong bài lab này, sinh viên sẽ sử dụng Wireshark và Tshark phiên bản 3.2.3

**Khởi động bài lab:**

- Vào terminal, gõ:

*labtainer ptit-network-tracing*

*(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)*

**Các nhiệm vụ:**

- Task 1: Lọc DNS

+ Thư mục hiện tại đã chuẩn bị sẵn một tệp tin .pcap để sinh viên phân tích. Để mở tệp tin này, sinh viên sử dụng lệnh sau:

*tshark -r test.pcap*

+ Như sinh viên thấy, màn hình sẽ xuất hiện toàn bộ các gói tin có trong tệp tin pcap. Nếu tệp tin này lớn hơn thì việc in ra màn hình là không thể. Vì thế, ta có thể sử dụng bộ lọc để đưa ra các gói tin cần thiết cho việc phân tích.

+ Để lọc gói tin DNS, sinh viên cần thêm lệnh *-Y "dns"* ngay đằng sau lệnh bên trên:

*tshark -r test.pcap -Y "dns"*

+ Sau khi áp dụng bộ lọc DNS, sinh viên chỉ sẽ thấy các gói tin DNS trong danh sách.

* Sinh viên hãy quan sát các gói tin DNS và ghi chú lại bất kỳ hoạt động bất thường nào.

- Task 2: Lọc HTTP.

+ Hiện nay đa số các web thông qua các giao thức an toàn trên cổng https/443 chứ không phải là http/80. Tuy nhiên, lưu lượng mạng tại đây lại xuất hiện khá nhiều gói tin trên cổng http/80, vì vậy chúng ta hãy tập trung vào nó và lọc các request/replies trên cổng 80 để biết xem các gói tin này sẽ đi đến đâu và các thông tin riêng tư có được mã hóa hay không. Sinh viên hãy dùng lệnh sau:

*tshark -r test.pcap -Y "http"*

+ Để xem sâu hơn về từng gói tin, sinh viên phải biết được thứ tự luồng TCP Stream của từng gói tin, để làm thế sinh viên có thể dùng lệnh sau:

*tshark -r test.pcap -Y "frame.number ==* ***20****" -T fields -e tcp.stream*

(frame.number chính là số thứ tự của gói tin trong luồng TCP ở cột đầu tiên của lệnh trước).

+ Tiếp theo, sinh viên hãy lọc các luồng TCP của yêu cầu GET đầu tiên xuất hiện trong tệp pcap (sinh viên hãy thay thế thứ tự luồng TCP Stream tìm được ở trên vào cuối lệnh, ở yêu cầu GET đầu tiên là “1”):

*tshark -r test.pcap -q -z "follow,tcp,ascii,****1****"*

* Sinh viên hãy cho biết yêu cầu GET này có gì khả nghi?

+ Sau đó, sinh viên hãy xem gói tin POST đầu tiên xuất hiện trong tệp tin .pcap này và trả lời câu hỏi sau:

*tshark -r test.pcap -q -z "follow,tcp,ascii,****8****"*

* Máy tính bị lây nhiễm đang cố gửi đi những gì?
* User-Agent và server có khác gì so với gói tin GET ở bước trước không?

- Task 3: Tìm kiếm vị trí địa lý của IP độc hại.

+ Ở luồng POST đầu tiên trong task trước, ta có thể thấy xuất hiện một địa chỉ ip lạ mà máy nạn nhân đang cố gửi đến. Wireshark phiên bản GUI có khả năng tìm vị trí địa lý của một địa chỉ IP thông qua một database. Tuy nhiên, sinh viên cần phải tự thêm database đó vào.

Mở wireshark → Chọn Edit → Chọn Preferenses → Chọn Name Resolution → Thêm database của GeoIP tại MaxMind database directories → Đẩy thư viện mới thêm lên đầu.

(Có thư mục database ở HOME, sinh viên hãy trỏ về thư mục đó).

+ Sau đó khởi động lại wireshark và trỏ về tệp test.pcap, sinh viên hãy tìm lại các gói tin http và tìm lại gói POST vừa nãy.

* Thông tin về địa chỉ địa lý xuất hiện ở “Internet Protocol Version 4”, sinh viên hãy cho biết địa chỉ IP lạ nằm ở khu vực nào?

- Task 4: Tìm kiếm tài khoản và mật khẩu.

+ Quay trở lại giao diện dòng lệnh, sinh viên hay tiếp tục xem luồng hoạt động http/post tiếp theo:

*tshark -r test.pcap -q -z "follow,tcp,ascii,****9****"*

+ Yêu cầu này sử dụng phương thức POST để gửi dữ liệu form-data đến máy chủ. Dữ liệu form này bao gồm hai trường "data" và "source". Trong một số trường hợp, việc gửi dữ liệu form như vậy có thể là một phần của các hành động độc hại hoặc tấn công, như gửi thông tin đăng nhập giả mạo hoặc dữ liệu nhạy cảm đến máy chủ.

* Hãy phân tích rõ gói tin này và cho biết máy nạn nhân đang cố gắng gửi thông tin gì đi?

+ Hãy tiếp tục mở 2 gói tin POST tiếp theo và ghi những gì tìm được vào báo cáo.

*tshark -r test.pcap -q -z "follow,tcp,ascii,****10****"*

*tshark -r test.pcap -q -z "follow,tcp,ascii,****11****"*

- Task 5: Lấy thông tin Hệ thống.

+ Ở nhiệm vụ này, sinh viên sẽ xem 2 gói tin POST cuối cùng xuất hiện trong tệp pcap. Trên terminal, sinh viên hãy chạy lệnh sau:

*tshark -r test.pcap -q -z "follow,tcp,ascii,****21****"*

*tshark -r test.pcap -q -z "follow,tcp,ascii,****85****"*

* Hãy cho biết có bao nhiêu tên máy khách xuất hiện trong gói tin này? Liệt kê username xuất hiện trong này.

- Task 6: Trích xuất tập tin EXE ẩn.

+ Qua các nhiệm vụ trên, nghi ngờ trong lưu lượng này có chứa tệp độc hại khá là cao. Đa số các tệp độc hại được cài đặt dưới dạng tệp tin thực thi .exe(windows) được ẩn mình thành các tệp khác để đánh lừa người dùng như: tệp hình ảnh,video, âm thanh,...

+ Để tìm kiếm các tệp tin này, sinh viên hãy dựa vào dấu hiệu của tệp thư thi là:

* MZ
* This program cannot be run in DOS mode
* …

+ Hãy lọc các gói tin có chứa những dấu hiện trên như sau:

*tshark -r test.pcap -Y "frame contains \"MZ\" && frame contains \"DOS\""*

* Gói tin được truyền qua cổng nào? Giao thức truyền tin là gì?

+ Có thể thấy rằng các gói tin này là một phần của một PDU (Protocol Data Unit) TCP được tái lập. Điều này chỉ ra rằng gói tin này là một phần của một dữ liệu lớn đã được chia nhỏ và gửi dưới dạng các phân đoạn TCP. Để tìm được chính xác dữ liệu đó được xử lý từ bao giờ và kết thúc ra sao, sinh viên hãy chạy lại lệnh:

*tshark -r test.pcap -Y "http"*

* Hãy cho biết số thứ tự bắt đầu và kết thúc trong luồng TCP của các gói tin vừa tìm thấy ở lệnh trước là gì?
* Mục đích của các gói tin này là gì?

+ Tiếp theo, sinh viên có thể trích xuất những tệp tin khả nghi này bằng cách sử dụng giao diện Wireshark:

Mở wireshark → Chọn File → Chọn Export Objects → Chọn HTTP…→ Chọn tệp tin cần trích xuất → Save.

(sinh viên hãy đặt tên file là: MSV\_STT.png)

(Ví dụ: B20DCAT999\_1.png)

+ Tuy nhiên, wireshark không phải công cụ có thể phân tích chuyên sâu về mã độc mà chỉ hỗ trợ trong việc theo dõi và lần vết các gói tin mà một máy bị nhiễm virus liên lạc với máy chủ C&C bên ngoài. Vì thế, sinh viên hãy tạo mã hash md5 từ 2 tệp tin vừa lưu được và gửi lên công cụ phân tích mã độc trực tuyến VirusTotal:

*md5sum <file>*

+ Tiếp theo, sinh viên hãy thực hiện kết nối đến 1 container khác bằng ssh thông qua lệnh sau:

*ssh ubuntu@192.168.0.20*

+ Mật khẩu chính là 1 trong 2 mã hash md5 mà sinh viên đã lấy được ở trên. Sau đó, hãy thực hiện in kết quả của tệp tin filetoview ra màn hình:

*cat filetoview*

**Kết thúc bài lab:**

- Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

*stoplab ptit-network-tracing*

- 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.

**Khởi động lại bài lab:**

- Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

*labtainer -r* *ptit-network-tracing*