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

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO BÀI TẬP LỚN**

**Chủ đề: Tìm hiểu về công cụ SiLK và ứng dụng SiLK trong việc phát hiện tấn công DOS**

Giảng viên: Hoàng Minh Thắng

Học phần: Kỹ thuật theo dõi và giám sát an toàn mạng

Thành viên nhóm 14 :

Đỗ Mạnh Hùng – B17DCAT087

Nguyễn Ngọc Bách – B17DCAT019

Bùi Xuân Duy – B17DCAT057

Nguyễn Thị Lụa – B17DCAT121

Triệu Tiến Đức – B17DCAT051

**MỤC LỤC**

**[MỤC LỤC 1](#_Toc19033)**

**[CHÚ THÍCH TỪ KHÓA 2](#_Toc19756)**

**[1. Giới thiệu về SiLK 3](#_Toc689)**

**[2. The SiLK Flow Repository 3](#_Toc4888)**

**[2.1. Bản ghi lưu lượng mạng 3](#_Toc20015)**

**[2.2. Tạo và thu thập lưu lượng mạng. 5](#_Toc6769)**

**[2.3. Nơi thu thập dữ liệu lưu lượng mạng 7](#_Toc13769)**

**[3. Bộ công cụ SiLK 8](#_Toc14682)**

**[4. Cách sử dụng SiLK để phân tích 9](#_Toc27657)**

**[4.1. Single-path Analysis 9](#_Toc8518)**

**[4.2. Multi-path Analysis 9](#_Toc18791)**

**[4.3. Exploratory Analysic (Phân tích thăm dò) 10](#_Toc10860)**

**[5. Quy trình làm việc để phân tích SiLK 11](#_Toc10319)**

**[5.1. Công thức(thu thập thông tin) 11](#_Toc1085)**

**[5.2. Bước](#_Toc1634) *[Model](#_Toc1634)* [13](#_Toc1634)**

**[5.3. Test 14](#_Toc14873)**

**[5.4. Phân tích 14](#_Toc15540)**

**[5.5. Lọc 14](#_Toc14097)**

**[5.6. Áp dụng quy trình làm việc SiLK 15](#_Toc28443)**

**[6. Demo cơ bản 15](#_Toc2186)**

**[6.1. Cài đăt SiLK 15](#_Toc4806)**

**[6.2. Phân tích SiLK 16](#_Toc24296)**

**[6.2.1. Thu thập thông tin 16](#_Toc11955)**

**[6.2.2. Model 18](#_Toc1202)**

**[6.2.3. Test 19](#_Toc19651)**

**[6.2.4. Phân tích 20](#_Toc2005)**

**[6.2.5. Tinh chỉnh 21](#_Toc2171)**

**[7. Demo phân tích tấn công Dos với SiLK và python 22](#_Toc28137)**

**[7.1. Giới thiệu môi trường lab 22](#_Toc20655)**

**[7.2. Các bước demo 22](#_Toc21409)**

**[Tài liệu tham khảo 28](#_Toc23468)**

**CHÚ THÍCH TỪ KHÓA**

|  |  |
| --- | --- |
| IP | Internet Protocol |
| SILK | System for Internet Level Knowledge |
| YAF2 | YY1-associated factor 2 |

## Giới thiệu về SiLK

- SiLK là phần mềm mã nguồn mở của nhóm Network Situational Awareness(Net SA) tại CERT để truy vấn và phân tích dữ liệu NetFlow. Bộ SiLK cho phép truy vấn nhanh chóng và hiệu quả lưu lượng mạng lớn theo thứ tự để xác định các hiện tượng phức tạp hoặc trích xuất các sự kiện riêng lẻ.

- SiLK thực sự là một cơ sở dữ liệu tại dòng lệnh. Mỗi công cụ thực hiện một truy vấn cụ thể, thao tác hoặc tổng hợp dữ liệu và các lệnh được kết nối với nhau để tạo ra các kết quả. Bằng cách kết nối nhiều bản ghi dọc theo đường ống, SiLK cho phép nhà phân tích tạo các lệnh phức tạp mà dữ liệu trường dọc theo nhiều kênh cùng một lúc.

## The SiLK Flow Repository

### Bản ghi lưu lượng mạng

NetFlow là một giao thức được phát triển bởi Cisco sử dụng để thu thập thông tin về lưu lượng truy cập qua các thiết bị mạng.Các thông tin thu thập thường bao gồm:Địa chỉ IP nguồn và đích,cổng nguồn và đích,giao thức lớp vận chuyển ,loại dịch vụ và giao diện bộ định tuyến.

SiLK sử dụng 5 thuộc tính sau để tạo dữ liệu lưu lượng mạng:

- Địa chỉ IP nguồn

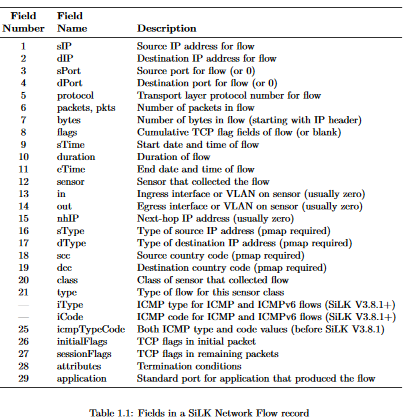
- Địa chỉ IP đích

- Cổng nguồn

- Cổng đích

- Giao thức lớp vận chuyển

Flow Record: bản ghi lưu lượng. Một bản ghi lưu lượng cung cấp nhãn và số liệu thống kê về các gói được bao phủ bởi luồng mạng,bao gồm luồng,tổng số byte,thời lượng và thời gian của các gói đó.Một tệp lưu lượng là một loạt các bản ghi lưu lượng.Bản ghi lưu lượng gồm các trường (bảng 1.1). Mỗi trường được xác định bởi một tên và số có thể sử dụng thay thế cho nhau.



Mỗi bản ghi lưu lượng tạo bởi SiLK là rất nhỏ ít nhât 22 byte nhưng một sensor có thể thu thập nhiều GB hồ sơ lưu lượng mạng ngày ngày trên một mạng bận rộn.

Một số trường được lưu trong hồ sơ như thời gian bắt đầu và thời lượng. Một số không được lưu trữ nó có nguốc từ thông tin trong trường lưu trữ hoặc kết hợp các trường được lưu trữ trong bản ghi và dữ liệu bên ngoài. Ví dụ: thời gian kết thúc được tính bằng cách thêm thời gian bắt đầu và thời lượng.Mã quốc gia nguồn được lấy từ địa chỉ IP nguồn và bảng ánh xạ địa chỉ IP thành mã quốc gia

### Tạo và thu thập lưu lượng mạng.

Dữ liệu được thu thập và hiển thị dưới dạng bản ghi lưu lượng mạng. Một bản ghi lưu lượng mạng được tạo bởi các cảm biến trên toàn mạng doanh nghiệp. Thông thường, phần lớn những cảm biến này là bộ định tuyến. Các cảm biến chuyên dụng như yaf[2](https://translate.googleusercontent.com/translate_f" \l "29) có thể được sử dụng khi nguồn cấp dữ liệu từ bộ định tuyến không có sẵn, chẳng hạn như trên mạng gia đình hoặc trên một máy chủ cá nhân. yaf cũng có thể được sử dụng để tránh hiện vật trong việc thực hiện lưu lượng mạng của bộ định tuyến hoặc sử dụng các định dạng dữ liệu lưu lượng mạng không dành riêng cho thiết bị như như IPFIX[3](https://translate.googleusercontent.com/translate_f" \l "30). Nó cung cấp thêm quyền kiểm soát đối với việc tạo bản ghi lưu lượng mạng và có thể chuyển đổi dữ liệu gói sang lưu lượng mạng ghi lại thông qua một tập lệnh tự động hóa quá trình này.

Một cảm biến tạo ra các bản ghi lưu lượng mạng bằng cách nhóm các gói có liên quan chặt chẽ với nhau theo thời gian và có nhãn lưu lượng chung. Có liên quan chặt chẽ với nhau được xác định bởi cảm biến và thường được đặt trong khoảng 30 giây.

Lưu lượng mạng là một xấp xỉ lưu lượng. Bộ định tuyến và các cảm biến khác đoán khi quyết định các gói thuộc về một luồng nào.Những phỏng đoán này không hoàn hảo; có một số hiện tượng nổi tiếng trong đó một phiên kéo dài sẽ được chia thành nhiều bản ghi lưu lượng:

*- Hết thời gian hoạt động* là nguyên nhân phổ biến nhất của luồng mạng bị chia. Hồ sơ lưu lượng mạng được thanh lọc từ bộ nhớ của cảm biến và được khởi động lại sau một thời gian hoạt động có thể định cấu hình. Kết quả là tất cả các mạng hồ sơ lưu lượng có giới hạn trên về thời lượng của chúng phụ thuộc vào cấu hình cục bộ. Một điển hình giá trị sẽ là khoảng 30 phút.

*- Xóa bộ đệm* là nguyên nhân phổ biến của các luồng mạng phân chia cho các bản ghi lưu lượng mạng được thu thập bởi bộ định tuyến. Mạng các luồng chiếm tài nguyên bộ nhớ trong bộ định tuyến và bộ định tuyến thường xuyên xóa bộ đệm mạng này dòng chảy cho mục đích vệ sinh. Việc xóa bộ nhớ cache diễn ra khoảng 30 phút một lần. Một chuỗi các luồng mạng trong một khoảng thời gian dài cho thấy nhiều luồng mạng chấm dứt đều đặn Khoảng thời gian 30 phút, là kết quả của việc xóa bộ đệm.

- *Sự* *cạn kiệt của bộ định tuyến* cũng gây ra các luồng mạng phân chia cho các luồng được thu thập bởi bộ định tuyến. Một bộ định tuyến có giới hạn tài nguyên xử lý và bộ nhớ dành cho lưu lượng mạng. Trong thời gian căng thẳng, bộ đệm lưu lượng sẽ lấp đầy và trống thường xuyên hơn do số lượng luồng mạng được thu thập bởi bộ định tuyến. Sử dụng các cảm biến lưu lượng chuyên dụng có thể tránh hoặc giảm thiểu các vấn đề cạn kiệt bộ đệm và bộ định tuyến. Tất cả những thứ ở đây các trường hợp liên quan đến các luồng mạng đủ dài để được phân chia. Như chúng tôi trình bày sau, phần lớn các luồng mạng thu thập tại biên giới mạng doanh nghiệp là nhỏ và ngắn hạn.

## Bộ công cụ SiLK

Bộ phân tích SiLK bao gồm hơn 60 công cụ UNIX dòng lệnh (bao gồm các công cụ thu thập luồng) nhanh chóng xử lý hồ sơ lưu lượng hoặc thao tác dữ liệu phụ trợ. Các công cụ có thể giao tiếp với nhau và với các công cụ kịch bản thông qua các đường ống (cả không tên và được đặt tên) hoặc qua các tệp trung gian

Phân tích SiLK thường bị ràng buộc đầu vào / đầu ra (ràng buộc I / O) Thời lượng cần thiết để thực hiện một phân tích tỷ lệ thuận với lượng dữ liệu đọc từ đĩa.

Mục tiêu chính của bộ công cụ SiLK là giảm thiểu thời gian truy cập đó Một số công cụ SiLK thực hiện các chức năng tương tự như dòng lệnh UNIX phổ biến các công cụ và các ngôn ngữ kịch bản cấp cao hơn như Perl. Tuy nhiên, các công cụ SiLK xử lý dữ liệu này trong dạng phi văn bản (nhị phân) và sử dụng các cấu trúc dữ liệu được tối ưu hóa đặc biệt để phân tích.

Do đó, hầu hết các phân tích SiLK bao gồm một chuỗi các hoạt động sử dụng các công cụ SiLK. Giữ dữ liệu nhị phân trong càng nhiều bước càng giúp cải thiện hiệu quả xử lý. Đây là vì các bản ghi nhị phân có cấu trúc được tạo bởi các công cụ SiLK có thể dễ dàng phân tách mà không cần phân tích cú pháp, các trường của chúng là nhỏ gọn và các trường đã ở định dạng sẵn sàng cho việc tính toán, chẳng hạn như tính toán mạng. Theo một số cách, thật phù hợp khi nghĩ về SiLK như một bộ công cụ nhận thức. Kho lưu trữ bản ghi cung cấp khối lượng dữ liệu lớn và bộ công cụ cung cấp các khả năng cần thiết để xử lý các dữ liệu này.

## Cách sử dụng SiLK để phân tích

Bộ công cụ SiLK cung cấp một bộ công cụ mạnh mẽ để tạo điều kiện thuận lợi cho các tác vụ phân tích lưu lượng mạng. Nó là được thiết kế để rất linh hoạt trong việc hỗ trợ các phương pháp phân tích. Theo thời gian, các nhà phân tích khác nhau đã sử dụng một nhiều cách tiếp cận trong việc sử dụng SiLK. Phần này thảo luận về ba phương pháp hữu ích trong phân tích hồ sơ lưu lượng mạng.

## Single-path Analysis

*Single-path analysis* là cách tiếp cận cơ bản nhất và được sử dụng phổ biến nhất để phân tích hành vi mạng. Nó sử dụng một chuỗi lệnh duy nhất để tạo ra kết quả phân tích. Theo cách tiếp cận này, nhà phân tích hình thành một giả thuyết ban đầu, xây dựng một truy vấn để lấy lưu lượng quan tâm, tạo ra một bảng, tóm tắt, hoặc loạt để lập hồ sơ lưu lượng này, và sau đó diễn giải hồ sơ này bằng số hoặc thông qua biểu đồ. Lặp lại có thể được sử dụng nếu cần (ví dụ: để tinh chỉnh truy vấn ban đầu), nhưng có thể không cần thiết cho nhiều đơn giản hơn, nhiều hơn phân tích đơn giản.

Cách tiếp cận này có thể được sử dụng để nhận dạng dịch vụ, kiểm kê thiết bị mạng, phản hồi sự cố hoặc sử dụng để học.

## Multi-path Analysis

*Multi-path analysis* sử dụng một chuỗi các công cụ thường liên quan đến một số lựa chọn thay thế và thường bao gồm lặp đi lặp lại qua một số bước. Mặc dù cách tiếp cận đa đường có thể được thực hiện thủ công, nhưng nó thường xuyên liên quan đến kịch bản để chọn các lựa chọn thay thế dựa trên các loại dữ liệu và sau đó lặp lại cho đến khi lưu lượng truy cập mong muốn là cô lập hoặc tóm tắt mong muốn được sản xuất. Các lựa chọn thay thế được sử dụng theo yêu cầu cho các nhóm xử lý hồ sơ theo những cách khác nhau để đạt được kết quả mà hồ sơ hành vi quan tâm.

Cách tiếp cận này có thể được sử dụng để kiểm tra lưu lượng sử dụng một số giao thức, mỗi giao thức theo sau thay thế của chính nó thiết lập các đặc điểm, để thực hiện cùng một mục tiêu. Ví dụ: có nhiều cách mà phần mềm độc hại có thể đèn hiệu vào mạng chỉ huy và kiểm soát của nó. Mỗi cách có thể được kiểm tra riêng thông qua một chuỗi các lệnh SiLK, tạo ra các tập hợp kết quả góp phần nhận thức tổng thể về đèn hiệu.

## Exploratory Analysis (Phân tích thăm dò)

Phân tích *thăm dò* là một cách tiếp cận mở để xây dựng, phân tích và tiến hành phân tích mạng. Nó sử dụng các phân tích một đường và nhiều đường như các khối xây dựng để điều tra sự bất thường lưu lượng mạng. Những loại phân tích đơn giản hơn này giúp chúng tôi xây dựng các kịch bản khác nhau, điều tra thay thế các giả thuyết và khám phá nhiều khía cạnh của dữ liệu. Phân tích thăm dò ban đầu là thủ công trong tự nhiên, nhưng có thể chuyển sang phân tích theo kịch bản để dễ lặp lại và cho kết quả đều đặn.

Cách tiếp cận này được sử dụng cho các hiện tượng phức tạp hoặc mới nổi, trong đó nhiều chỉ số cần được kết hợp để đạt được sự hiểu biết. Một ví dụ về phương pháp phân tích này sẽ là một nghiên cứu về việc lọc dữ liệu, trong đó có thể được thực hiện theo nhiều cách khác nhau. Mỗi phương thức tẩy tế bào chết có thể được định hình bằng cách sử dụng một bộ về các chỉ số và kết quả của tất cả các phân tích như vậy được kết hợp để tạo ra sự hiểu biết tổng hợp về lưu lượng truy cập được chuyển đến các nhóm địa chỉ đáng ngờ khác nhau.

1. **Cài đặt SiLK**

* Tải tệp cấu hình và cài đặt SiLK theo địa chỉ:

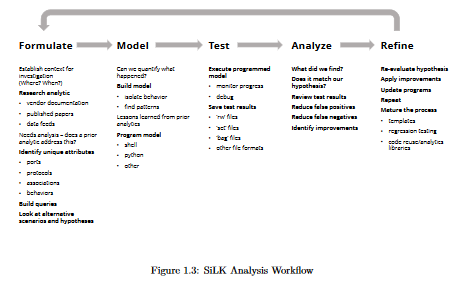
wget https://raw.githubusercontent.com/chrissanders/FlowBAT/master/support/silkonabox.sh

* Gán quyền để thực thi tệp với lệnh: chmod +x silkonabox.sh và chạy lệnh sau để cài đặt: ./silkonabox.sh
* Sau khi cài đặt thành công ta sẽ thu được kết quả và version của SiLK :

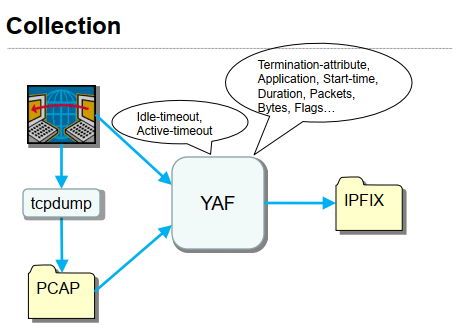


## Quy trình làm việc để phân tích SiLK

Các phân tích SiLK chia sẻ một quy trình công việc chung. Trong khi đường đơn, đa đường và thám hiểm phân tích có thể kết hợp các bước khác nhau trong quy trình công việc này, tất cả đều tuân theo trình tự chung của nó.



### Formulate



Bước *Formulate* điều tra bối cảnh của sự kiện. Về cơ bản, nó liên quan đến việc thu thập thông tin để xác định các thuộc tính duy nhất của mạng, hoạt động của nó và sự kiện. Mạng lưới rộng bao nhiêu? Thế nào là nó có cấu trúc? Cảm biến mạng được đặt ở đâu? Sự kiện này xảy ra khi nào? Có liên quan đến cụ thể đến cảm biến, địa chỉ IP, máy chủ, không gian mạng, cổng, giao thức, v.v. Làm bất kỳ phân tích trước đó của Mạng lưới cung cấp cái nhìn sâu sắc? Thông tin có thể không đầy đủ tại thời điểm này, nhưng nó đóng vai trò là điểm khởi đầu cho đưa ra các phân tích và thiết lập phạm vi của nó. Chúng ta có thể sử dụng nó để hình thành một giả thuyết cho hành vi mạng. Chúng ta có thể hình thành nhiều kịch bản và giả thuyết để điều tra và phân tích.

Thông tin lượm lặt được từ việc khám phá bối cảnh của sự kiện giúp chúng ta thiết lập các hành vi mạng nào nên được bao gồm trong (hoặc loại trừ khỏi) phân tích của chúng tôi. Chúng ta có thể sử dụng thông tin này để xây dựng một *truy vấn* để chọn và các bản ghi lưu lượng mạng phân vùng từ kho lưu trữ SiLK hoặc một tệp được lưu trữ. Truy vấn thường kết hợp thông tin như nơi lưu lượng được thu thập, ngày thu thập dữ liệu và hướng lưu lượng. Trong cộng đồng SiLK, lựa chọn truy vấn thường được gọi là *kéo dữ liệu* *Phân vùng* áp dụng các thử nghiệm cho các bản ghi lưu lượng được chọn để phân tách (hoặc phân vùng) chúng thành các danh mục để biết thêm kiểm tra, điều tra. Một bộ thử nghiệm mặc định được cung cấp với SiLK. Nó bao gồm địa chỉ IP, cổng, giao thức, thời gian và khối lượng. (Nếu các thử nghiệm bổ sung là cần thiết để phân tích, các công cụ SiLK có thể được mở rộng thông qua các *plugin* để cung cấp cho họ.)

Sự kết hợp giữa lựa chọn và phân vùng (thường được gọi là *lọc* ) được thực hiện với lệnh rwfilter. Các hồ sơ đáp ứng các tiêu chí lọc được gửi để *vượt qua* các điểm đến. Hồ sơ làm không được gửi đến các điểm đến *thất bại* . Cả hai có thể được kết hợp vào *tất cả các* điểm đến. Điều này cung cấp các tùy chọn linh hoạt để lưu trữ kết quả truy vấn trong tệp hoặc sử dụng đường ống để gửi chúng đến các lệnh khác để xử lý.

### *Model*

Bước model tóm tắt dữ liệu và điều tra các hành vi quan tâm. Hành vi của mạng là gì trong quá trình hoạt động bình thường? Điều gì đã xảy ra trong một sự kiện? Những mô hình và hành vi chúng ta có thể xác định? Chúng có giống với những gì được quan sát trong các sự kiện khác không? Bằng cách kiểm tra thông tin thu thập được trong Formulate , bạn có thể đưa ra một mô hình của sự kiện có lẽ giải thích những gì đang diễn ra.

SiLK cung cấp nhiều công cụ để kiểm tra dữ liệu lưu lượng mạng liên quan đến một sự kiện. Mỗi công cụ đưa ra các quan điểm khác nhau về dữ liệu có thể được xem xét độc lập hoặc kết hợp để phân tích.

Ví dụ: SiLK bao gồm các công cụ để tạo tổng kết lưu lượng theo chuỗi thời gian (lệnh rwcount), thống kê tóm tắt điện toán (lệnh rwstats) và tổng hợp các giá trị của các thuộc tính luồng cho khoảng thời gian do người dùng định nghĩa (lệnh rwuniq). Bước này có thể được thực hiện bằng tay. Đối với các phân tích có phạm vi lớn hơn, nó có thể được tự động hóa bằng cách sử dụng shell hoặc tập lệnh Python

### Test

Bước *Kiểm tra* chạy mô hình mà bạn đã tạo ra bằng tay hoặc bằng cách thực thi các tập lệnh shell hoặc Python. Điều này cung cấp cho bạn một cơ hội để kiểm tra tiến trình phân tích. SiLK bao gồm các lệnh để sắp xếp các bản ghi lưu lượng theo các khóa do người dùng xác định (lệnh rwsort), tạo tập hợp các địa chỉ IP duy nhất từ các bản ghi lưu lượng (rwset và các lệnh liên quan của nó) và tạo các nhóm bản ghi theo các tiêu chí khác (rwbag và các lệnh liên quan của nó). Các lệnh này giúp bạn tổ chức xuất ra từ các lệnh SiLK khác nhau và lưu nó để sử dụng tiếp.

### Analyze

Bước *Phân tích* xem xét kết quả của các bước trước. Những kết quả này cho chúng ta biết gì về sự kiện này? Những hành vi đã được xác định? Những loại sự kiện họ liên quan đến? Những mối quan hệ chúng ta có thể xác định giữa các dòng chảy? Các giả thuyết ban đầu của chúng tôi vẫn còn giữ? Chúng ta có thể tìm và loại bỏ sai tích cực và tiêu cực sai?

Bước này bao gồm kiểm tra và giải thích đầu ra từ các công cụ phân tích được đề cập trước đó. SiLK cũng có thể dịch các bản ghi lưu lượng nhị phân thành văn bản để phân tích với các gói đồ họa, bảng tính và toán học công cụ (lệnh rwcut).

### Refine

Bước *Tinh chỉnh* cải thiện phân tích. Chúng tôi đã giải thích thành công sự kiện này? Nếu không, chúng ta đã có gặp gỡ vấn đề gì? Chúng tôi đã hiểu đúng bối cảnh của sự kiện? Có phải truy vấn của chúng tôi vào kho lưu trữ SiLK quá nhiều dữ liệu? Chúng ta có cần đào sâu vào dữ liệu trong các bước thử nghiệm và mô hình hóa không? Chúng ta có nên hãy xem xét lại các kết quả để xem liệu chúng ta có bỏ lỡ hoặc giải thích sai các mô hình và hành vi quan trọng không?

Các bước trước trong quy trình làm việc có thể được kết hợp theo mô hình lặp. Ví dụ, bạn có thể muốn cô lập các bản ghi lưu lượng quan tâm khỏi lưu lượng mạng không liên quan bằng cách thực hiện các truy vấn bổ sung với lệnh rwfilter và lặp lại các bước tiếp theo trong phân tích. Điều này thu hẹp dữ liệu để tập trung vào các khoảng thời gian và các hành vi quan tâm và loại bỏ các hồ sơ lưu lượng không cần thiết.

Quy trình công việc được mô tả trong phần này cung cấp cho chúng tôi tính linh hoạt để bắt đầu khám phá dữ liệu của chúng tôi với một tổng quát câu hỏi, áp dụng một hoặc nhiều phân tích cho câu hỏi và hoàn thành quy trình công việc với một phân tích lặp lại.

Tuy nhiên, sự linh hoạt này đi kèm với sự đánh đổi. Các truy vấn thường tăng tỷ lệ thuận với thời gian cửa sổ và lưu lượng ghi thuộc tính của một phân tích. Do đó, một mô hình chính xác của một phân tích nên được được sản xuất để giảm thiểu kết quả truy vấn.

### Áp dụng quy trình làm việc SiLK

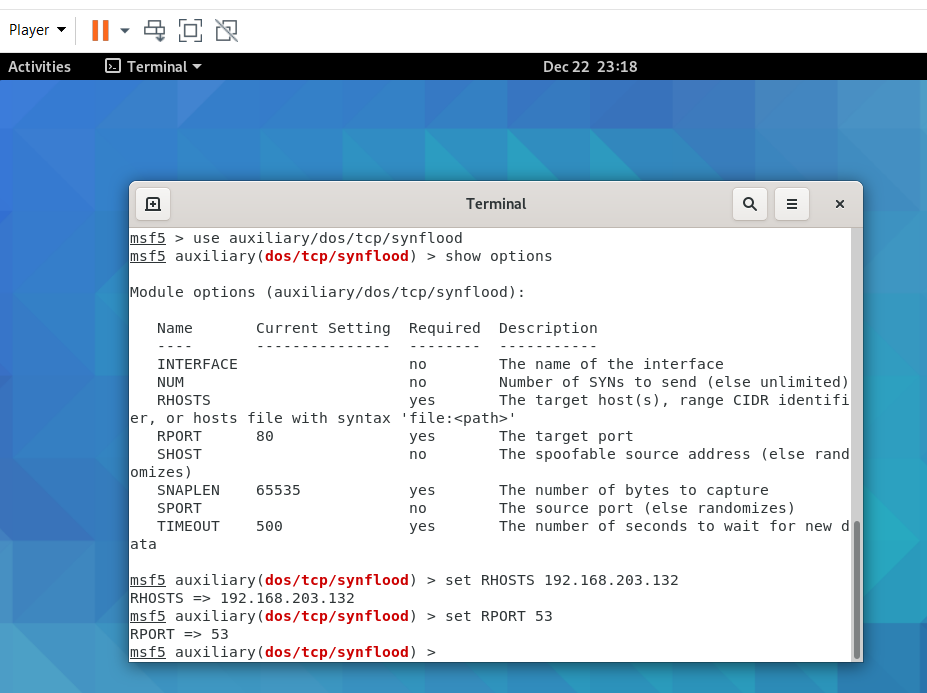
Quy trình công việc SiLK có thể được áp dụng theo các cách khác nhau để đáp ứng các yêu cầu của các nhóm phân tích. Các nhóm mà chủ yếu liên quan đến hoạt động mạng thường sẽ tập trung vào giám sát hoặc dịch vụ mạng và xác nhận thiết bị. Các nhóm phản ứng sự cố thường tập trung vào những thay đổi trong hành vi mạng có thể là liên quan đến một sự cố. Các nhóm cải tiến bảo mật thường tập trung vào việc hiểu mạng có vấn đề hành vi và thay đổi xác định tác động của cải tiến. Mặc dù bộ SiLK cung cấp các tính năng hỗ trợ tất cả các nhóm, công việc cần thiết để sử dụng chúng sẽ khác nhau.

1. **Demo phân tích tấn công Dos với SiLK và python**
   1. **Giới thiệu môi trường lab**

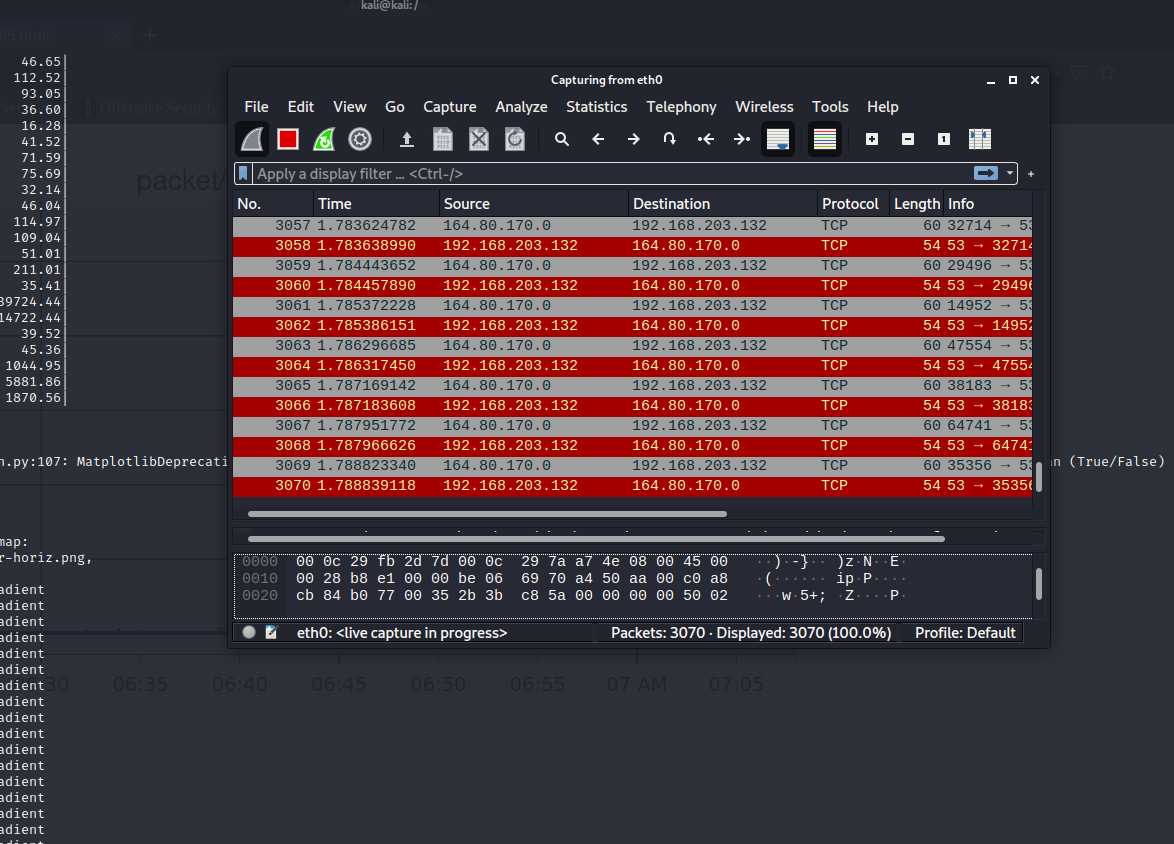
Môi trường lab gồm 2 máy ảo cài trên vm ware, 1 máy ảo tấn công cài metasploit để tấn công dos, 1 máy ảo nạn nhân cài silk

* 1. **Các bước demo**

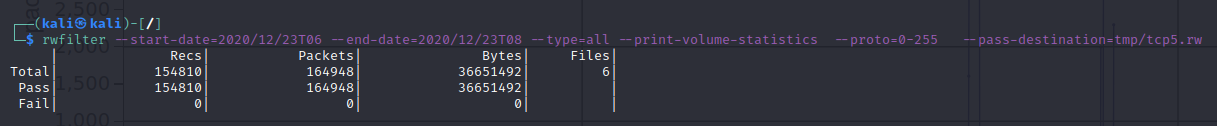
Khởi tạo và cấu hình metasploit ở máy tấn công



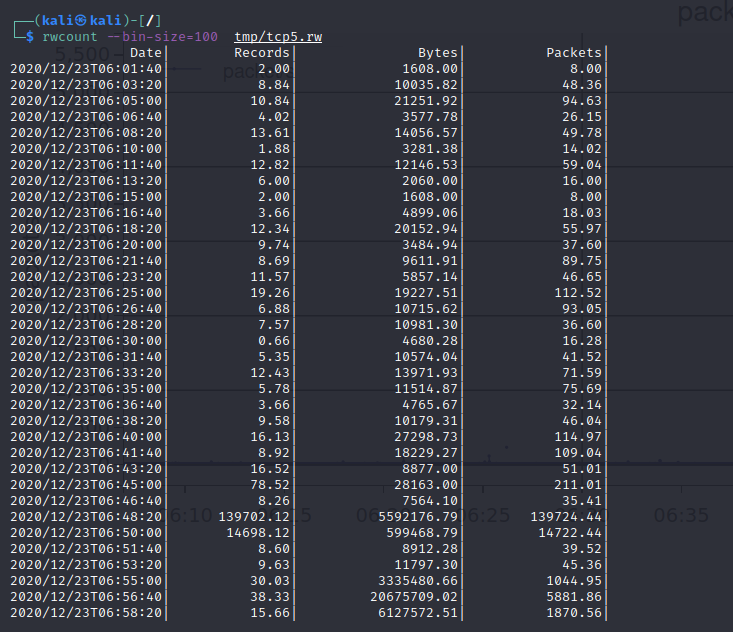
* Test tấn công thành công bằng wireshark ở máy nạn nhân



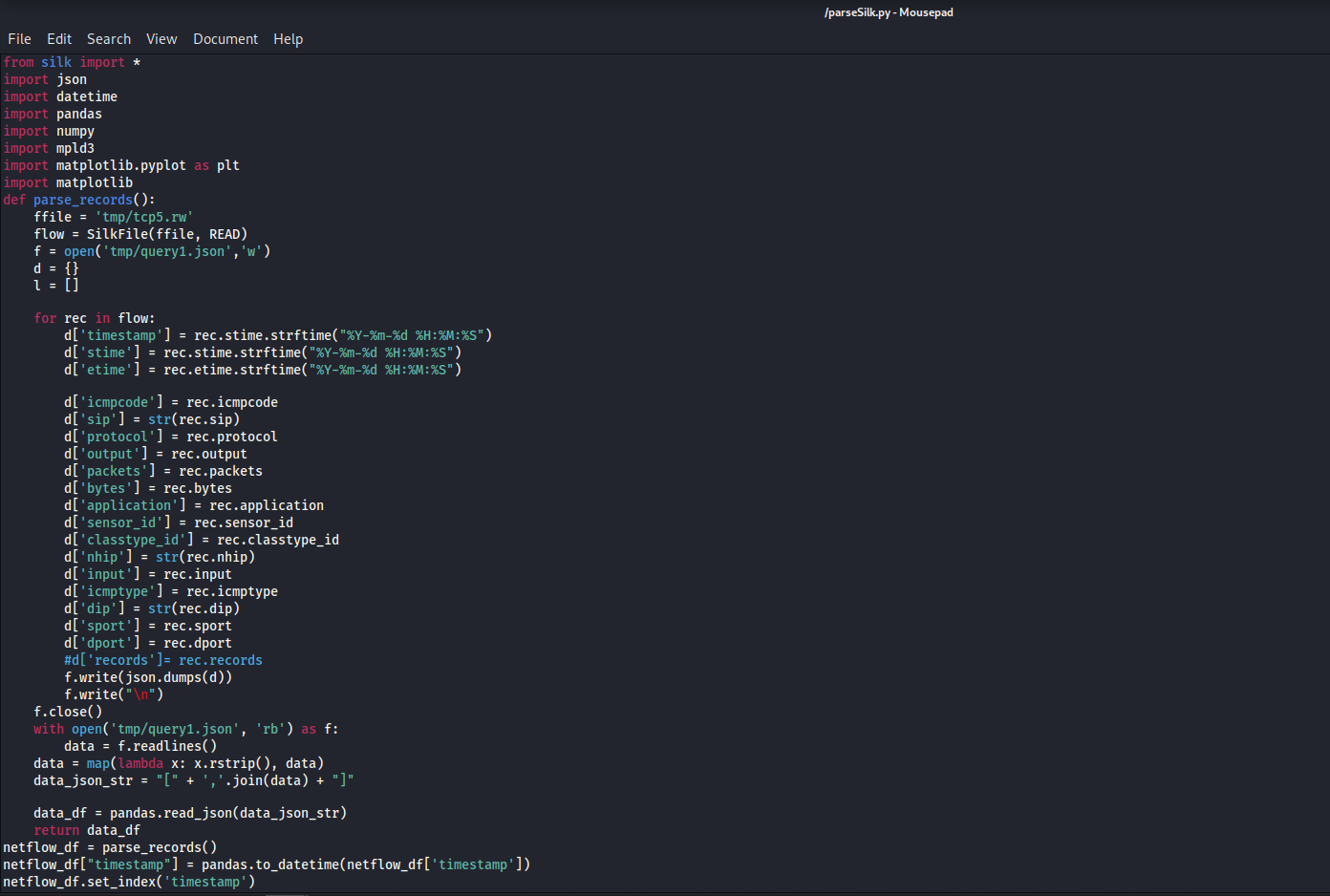
* Thu thập bản ghi netflow ứng với thời gian vừa tấn công dos ra bản ghi tcp5.rw



* Truy vấn số bản ghi theo thời gian qua lệnh rwcount

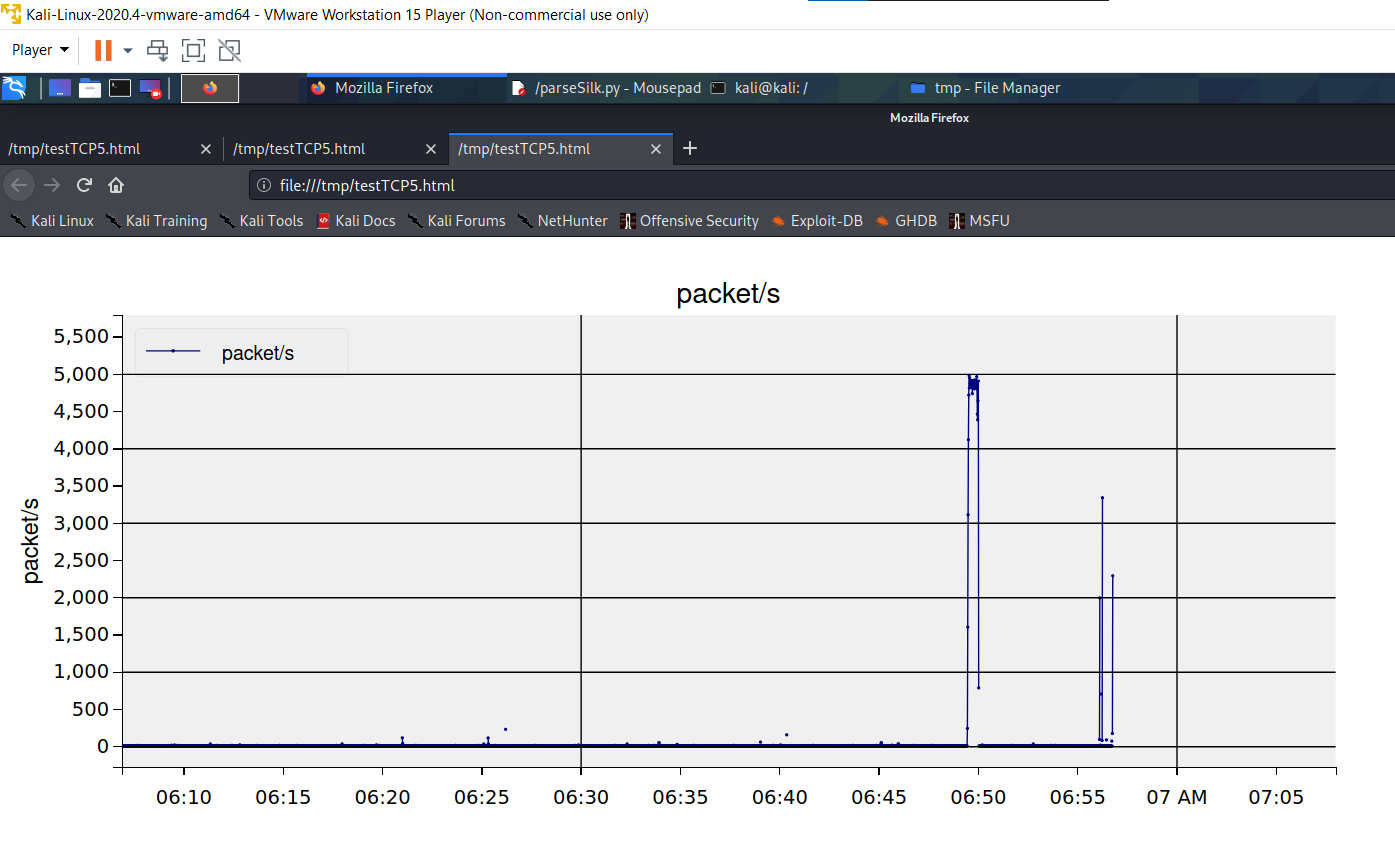


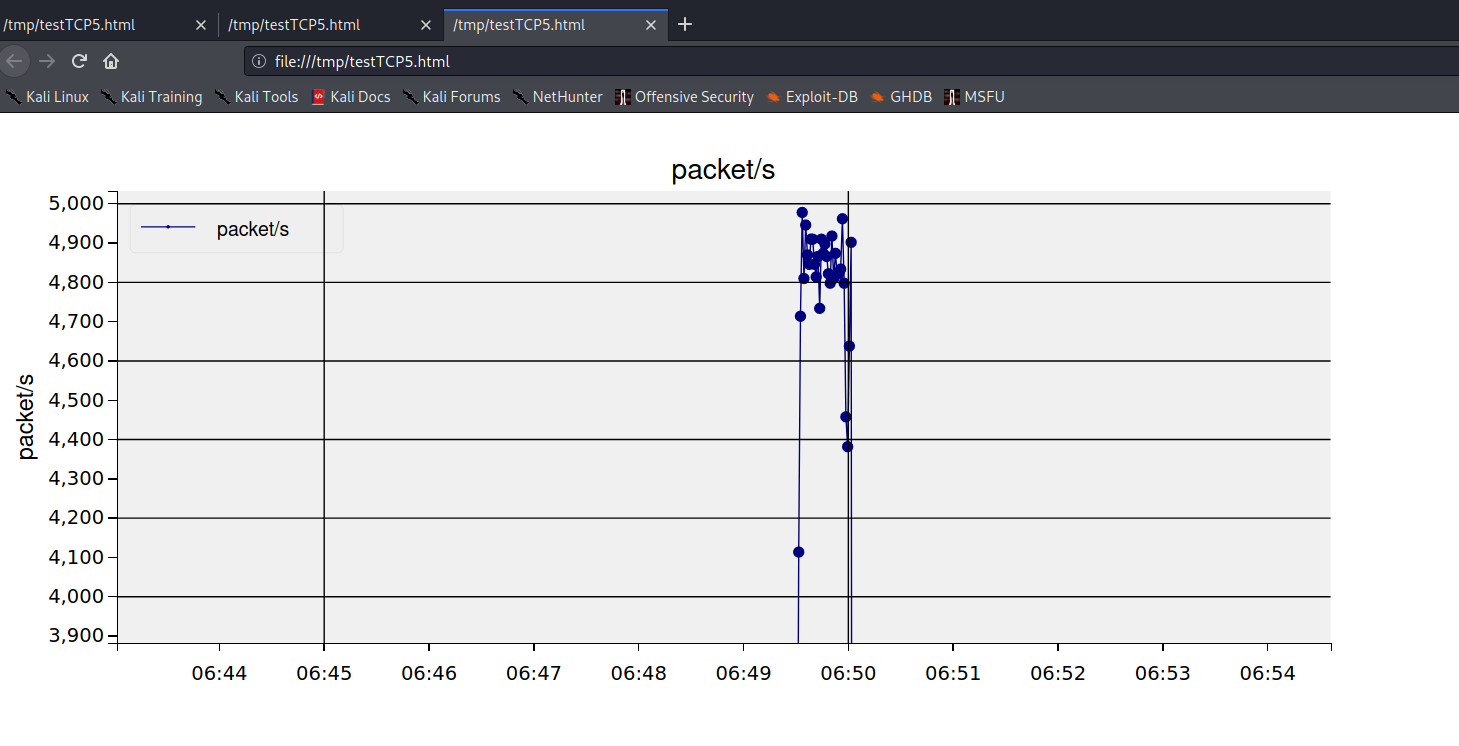
* Parse dữ liệu bản ghi ra json bằng thư viện silk trong python, rồi từ file json thư viện pyplot sẽ render ra biểu đồ tùy theo cấu hình và mục đích phân tích. Cụ thể với tấn công dos, sẽ lựa chọn thông số packet/s để phân tích tấn công.





* Kết quả ra file testTCP5.html





Từ biểu đồ chúng ta có thể sử dụng vào phân tích cuộc tấn công Dos

# **Tài liệu tham khảo**

- https://learning.oreilly.com/library/view/network-security-through/9781449357894/ch05.html

- https://tools.netsa.cert.org/silk/analysis-handbook.pdf

- http://www.flowbat.com/installation.html

- https://blog.because-security.com/t/netflow-data-analysis-with-silk-and-pandas/86