DOI: 10.62829/VNHN.366.69.74

GIÁM SÁT AN NINH MẠNG BẰNG PHƯƠNG PHÁP PHÂN TÍCH TỆP TIN NHẬT KÝ HỆ THỐNG

✍**Văn Thiên Hoàng - Nguyễn Trọng Minh Hồng Phước - Nguyễn Hoàng Duy**
Trường Đại học Quốc tế Sài Gòn

● **TÓM TẮT:** *Giám sát an ninh mạng ngày càng được quan tâm nghiên cứu và áp dụng cho việc theo dõi một hệ thống mạng máy tính, xem xét các thành phần hoạt động chậm lại hoặc không hoạt động và thông báo cho quản trị viên về các mối đe doạ từ bên ngoài hoặc các vấn đề gây ra bởi các máy chủ bị quá tải, hư hỏng. Từ đó, người quản trị hệ thống sẽ có các biện pháp giải quyết sự cố, phòng ngừa và ngăn chặn những hành vi xâm nhập mạng trái phép. Phương pháp phân tích tệp tin nhật ký hệ thống đóng vai trò quan trọng trong việc giám sát an ninh mạng. Bài báo đã đề cập đến việc giám sát an ninh mạng bằng phương pháp phân tích tệp tin nhật ký hệ thống. Các kết quả thực nghiệm minh chứng phương pháp đề xuất cho hiệu năng thực hiện cao, cả về độ chính xác và thời gian xử lý.*

● ***Từ khóa:*** *Giám sát mạng, tệp tin nhật ký, an ninh mạng.*

● **ABSTRACT:** *Network security monitoring is increasingly being researched and applied for monitoring a computer network, considering which component is slow down or inactive and informing administrators about external threats or problems caused by overloaded or damaged servers. Since then, the system administrator will take measures to resolve incidents, prevent acts of unauthorized network intrusion. The method of analyzing system log files plays an important role in monitoring network security. The article mentioned the monitoring of network security by analyzing the system log file. The experimental results demonstrate the proposed method for high performance, both in terms of accuracy and processing time.*

● ***Keywords:*** *network monitoring, log files, network security.*

Ngày nhận bài: 23/6/2025 Ngày bình duyệt: 04/7/2025 Ngày duyệt đăng: 10/7/2025

GIỚI THIỆU

Giám sát an ninh mạng sử dụng nhiều loại dữ liệu khác nhau để phát hiện, xác minh và khai thác. Nhiệm vụ chính của việc phân tích an ninh mạng là xác minh thành công hoặc cố gắng khai thác bằng cách sử dụng dữ liệu và công cụ giám sát an ninh mạng.

Điều tra số [1] là sự phục hồi và điều tra thông tin tìm thấy trên các thiết bị kỹ thuật số vì nó liên quan đến hoạt động tội phạm. Thông tin này có thể là dữ liệu trên các thiết bị lưu trữ, trong bộ nhớ điện tĩnh của máy tính hoặc dấu vết của tội phạm mạng được lưu giữ trong dữ liệu mạng, chẳng hạn như tệp tin pcaps và tệp tin nhật ký.

Các nhà phân tích an ninh mạng có thể thấy mình tiếp xúc trực tiếp với bằng chứng điều tra số chi tiết về hành vi của các thành viên trong tổ chức. Các nhà phân tích phải biết các yêu cầu liên quan đến việc bảo quản và xử lý các bằng chứng đó. Không làm như vậy có thể dẫn đến hình phạt hình sự cho tổ chức và thậm chí các nhà phân tích an ninh mạng nếu ý định phá hủy bằng chứng được thiết lập.

Security Onion [2] là bộ công cụ mã nguồn mở của các công cụ giám sát an ninh mạng chạy trên nền tảng Ubuntu Linux. Security Onion có thể được cài đặt độc lập hoặc dưới dạng nền tảng máy chủ. Một số thành phần của Security Onion được sở hữu và bảo trì bởi các tập đoàn, chẳng hạn như Cisco và Riverbend Technologies, nhưng được cung cấp dưới dạng nguồn mở.

Mối đe dọa liên tục thay đổi khi các lỗ hổng mới được phát hiện và các mối đe dọa mới phát triển. Khi người dùng và tổ chức thay đổi, phương thức tấn công cũng vậy. Các tác nhân đe dọa đã học được cách nhanh chóng thay đổi các tính năng khai thác của nó để tránh bị phát hiện.

Không thể thiết kế các biện pháp để ngăn chặn tất cả các khai thác. Khai thác chắc chắn sẽ trốn tránh các biện pháp bảo vệ, bất kể chúng có thể tinh vi đến mức nào. Đôi khi, điều tốt nhất có thể được thực hiện là phát hiện các khai thác trong hoặc sau khi chúng đã xảy ra. Nói cách khác, tốt hơn là có các cảnh báo đôi khi được tạo ra bởi lưu lượng truy cập không gây hại, hơn là có các quy tắc bỏ lỡ lưu lượng độc hại. Vì lý do này, cần phải có các nhà phân tích an ninh mạng lành nghề điều tra các cảnh báo để xác định xem một vụ khai thác có thực sự xảy ra hay không.

2. PHƯƠNG PHÁP PHÂN TÍCH

Phần này trình bài các phần của việc giám sát hệ thống mạng bằng phương pháp phân tích tệp tin nhật ký hệ thống.

2.1. Tệp tin nhật ký (Log file):

Log là phần mở rộng tệp cho một tệp được tạo tự động có chứa bản ghi các sự kiện từ một số phần mềm và hệ điều hành nhất định. Mặc dù chúng có thể chứa một số thứ, các tệp nhật ký thường được sử dụng để hiển thị tất cả các sự kiện liên quan đến hệ thống hoặc ứng dụng đã tạo ra chúng [3].

Điểm quan trọng của tệp nhật ký là theo dõi những gì xảy ra trong hậu trường và nếu có chuyện gì xảy ra trong một hệ thống phức tạp, bạn có quyền truy cập vào danh sách chi tiết các sự kiện diễn ra trước sự cố.

2.2. Các loại dữ liệu trên mạng:

Dữ liệu phiên [4] là bản ghi cuộc hội thoại giữa hai điểm cuối mạng, thường là máy khách và máy chủ. Máy chủ có thể ở trong mạng doanh nghiệp hoặc tại một địa điểm được truy cập qua Internet. Dữ liệu phiên là dữ liệu về phiên, không phải dữ liệu được khách hàng truy xuất và sử dụng. Dữ liệu phiên sẽ bao gồm thông tin nhận dạng, chẳng hạn như bộ địa chỉ IP nguồn và đích, số cổng nguồn và đích và mã IP cho giao thức được sử dụng. Dữ liệu về phiên thường bao gồm ID phiên, lượng dữ liệu được truyền theo nguồn và đích và thông tin liên quan đến thời lượng của phiên.

Dữ liệu giao dịch [5] bao gồm các tin nhắn được trao đổi trong các phiên mạng. Nhật ký thiết bị được giữ bởi máy chủ cũng chứa thông tin về các giao dịch xảy ra giữa máy khách và máy chủ. Các giao dịch thể hiện các yêu cầu và trả lời sẽ được ghi vào nhật ký truy cập trên máy chủ. Phiên là tất cả lưu lượng truy cập liên quan đến việc tạo ra yêu cầu, giao dịch là chính yêu cầu.

Giống như dữ liệu phiên, dữ liệu thống kê [6] là về lưu lượng mạng. Dữ liệu thống kê được tạo ra thông qua việc phân tích các dạng dữ liệu mạng khác. Từ những phân tích này, các kết luận có thể được đưa ra để mô tả hoặc dự đoán hành vi mạng. Các đặc điểm thống kê về hành vi mạng bình thường có thể được so sánh với lưu lượng mạng hiện tại trong nỗ lực phát hiện sự bất

thường. Thống kê có thể được sử dụng để mô tả số lượng biến thể thông thường trong các mẫu lưu lượng mạng để xác định các điều kiện mạng nằm ngoài phạm vi đó. Sự khác biệt có ý nghĩa thống kê sẽ tăng báo động và điều tra kịp thời.

Phân tích hành vi mạng (NBA) và Phát hiện bất thường hành vi mạng (NBAD) là các phương pháp tiếp cận giám sát an ninh mạng sử dụng các kỹ thuật phân tích nâng cao để phân tích dữ liệu từ xa của NetFlow (Cisco) hoặc Xuất thông tin giao thức Internet (IPFIX). Các kỹ thuật như phân tích dự đoán và trí tuệ nhân tạo thực hiện các phân tích nâng cao về dữ liệu phiên chi tiết để phát hiện các sự cố bảo mật tiềm ẩn [7].

2.3. Điều tra dữ liệu mạng:

Nhiệm vụ chính của một nhà phân tích an ninh mạng là xác minh các cảnh báo bảo mật. Tùy thuộc vào tổ chức, các công cụ được sử dụng để làm điều này sẽ khác nhau. Ví dụ, một hệ thống bán vé có thể được sử dụng để quản lý tài liệu và phân công nhiệm vụ. Trong Security Onion, nơi đầu tiên mà một nhà phân tích an ninh mạng sẽ đến để xác minh cảnh báo là Sguil.

Sguil [8] tự động tương quan các cảnh báo tương tự thành một dòng duy nhất và cung cấp một cách để xem các sự kiện tương quan được đại diện bởi dòng đó. Để hiểu được những gì đã xảy ra trong mạng, có thể hữu ích khi sắp xếp trên cột CNT để hiển thị các cảnh báo với tần suất cao nhất.

Sguil cung cấp khả năng cho nhà phân tích an ninh mạng xoay quanh các nguồn thông tin và công cụ khác. Các tệp nhật ký có sẵn trong ELSA, các gói chụp có liên quan có thể được hiển thị trong Wireshark và bản sao các phiên TCP và thông tin Bro cũng có sẵn.

Ngoài ra, Sguil có thể cung cấp độ tin cậy cho Hệ thống phát hiện tài nguyên thời gian thực thụ động (PRADS) [9] và thông tin cấu hình mạng phân tích bảo mật (SANCP) [10].

PRADS thu thập dữ liệu hồ sơ mạng, bao gồm thông tin về hành vi của tài nguyên trên mạng. PRADS là một nguồn sự kiện, như Snort và OSSEC. Nó cũng có thể được truy vấn thông qua Sguil khi một cảnh báo cho biết rằng một máy chủ nội bộ có thể đã bị xâm phạm. Thực hiện truy vấn PRADS từ Sguil có thể cung cấp thông tin về các dịch vụ, ứng dụng và tải trọng có thể liên quan đến cảnh báo. Ngoài ra, PRADS phát hiện khi tài sản mới xuất hiện trên mạng.

2.4. Biểu ngữ hình thức:

AWK [11] là ngôn ngữ lập trình được thiết kế để thao tác với các tệp văn bản. Nó rất mạnh mẽ và đặc biệt hữu ích khi xử lý các tệp văn bản trong đó các dòng chứa nhiều trường, được phân tách bằng ký tự phân cách. Các tệp nhật ký chứa một mục nhập trên mỗi dòng và được định dạng dưới dạng các trường được phân tách bằng dấu phân cách, làm cho AWK trở thành một công cụ tuyệt vời để chuẩn hóa.

2.5. Phân tích xác định và phân tích xác suất:

Các kỹ thuật thống kê có thể được sử dụng để đánh giá rủi ro khai thác thành công trong một mạng nhất định. Kiểu phân tích này có thể giúp những người ra quyết định đánh giá tốt hơn chi phí giảm thiểu mối đe dọa với thiệt hại mà việc khai thác có thể gây ra.

Hai cách tiếp cận chung được sử dụng để làm điều này là phân tích xác định và xác suất. Phân tích xác định [12] đánh giá rủi ro dựa trên những gì đã biết về lỗ hổng. Nó giả định rằng để khai thác thành công, tất cả các bước trước trong quy trình khai thác cũng phải thành công. Loại phân tích rủi ro này chỉ có thể mô tả trường hợp xấu nhất. Tuy nhiên, nhiều tác nhân đe dọa, mặc dù nhận thức được quá trình thực hiện khai thác, có thể thiếu kiến thức hoặc chuyên môn để hoàn thành thành công từng bước trên con đường dẫn đến khai thác thành công. Điều

này có thể cung cấp cho các nhà phân tích an ninh mạng một cơ hội để phát hiện khai thác và ngăn chặn nó trước khi nó tiến hành thêm nữa.

Phân tích xác suất [13] ước tính thành công tiềm năng của một khai thác bằng cách ước tính khả năng nếu một bước trong khai thác được hoàn thành thành công thì bước tiếp theo cũng sẽ thành công. Phân tích xác suất đặc biệt hữu ích trong phân tích bảo mật mạng thời gian thực, trong đó có nhiều biến số đang diễn ra và một tác nhân đe dọa nhất định có thể đưa ra quyết định chưa biết khi khai thác được theo đuổi.

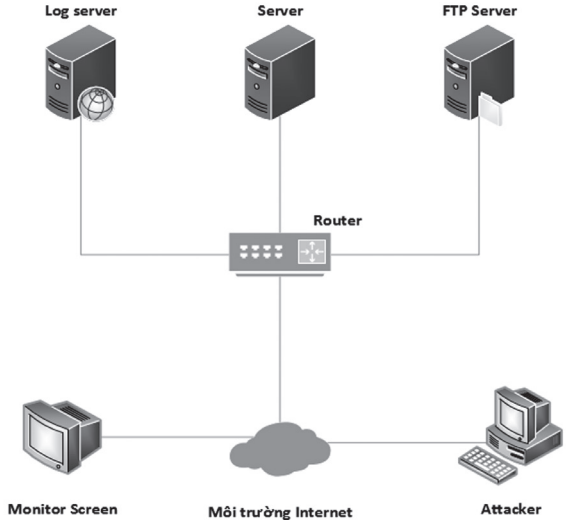
Phân tích xác suất dựa trên các kỹ thuật thống kê được thiết kế để ước tính khả năng xảy ra sự kiện dựa trên khả năng các sự kiện trước đó sẽ xảy ra. Sử dụng loại phân tích này, các con đường có khả năng khai thác nhất có thể được ước tính và sự chú ý của nhân viên an ninh có thể được tập trung vào việc ngăn chặn hoặc phát hiện khả năng khai thác.

Trong một phân tích xác định, tất cả các thông tin để thực hiện khai thác được giả định là đã biết. Các đặc điểm của khai thác, chẳng hạn như việc sử dụng số cổng cụ thể, được biết đến từ các trường hợp khai thác khác hoặc do các cổng được tiêu chuẩn hóa đang được sử dụng. Trong phân tích xác suất, người ta cho rằng số cổng sẽ được sử dụng chỉ có thể được dự đoán với một mức độ tin cậy nào đó. Trong tình huống này, một khai thác sử dụng số cổng động, chẳng hạn, không thể được phân tích một cách xác định. Khai thác như vậy đã được tối ưu hóa để tránh bị phát hiện bởi tường lửa sử dụng quy tắc tĩnh.

3. KẾT QUẢ THỰC NGHIỆM

Chương này trình bày các kết quả thực nghiệm của phương pháp đề xuất. Phương pháp đề xuất được thực nghiệm trên tảng ảo hoá từ phần mềm Orcale VM VirutalBox, với hai máy tính tham gia vào mô hình là CyberOps Workstation và Metaploit.

3.1. Mô hình thực nghiệm:



Chuyển đường dẫn truy cập bằng lệnh **cd** đến thư mục **/home/analyst/lab.support.files/**

```
[analyst@secOps lab.support.files]$ ls -l
total 580
-rw-r--r-- 1 analyst analyst     649 Mar 21  2018 apache_in_epoch.log
-rw-r--r-- 1 analyst analyst     126 Mar 21  2018 applicationX_in_epoch.log
drwxr-xr-x 4 analyst analyst    4096 Mar 21  2018 attack_scripts
-rw-r--r-- 1 analyst analyst     102 Mar 21  2018 confidential.txt
-rw-r--r-- 1 analyst analyst    2871 Mar 21  2018 cyops.mn
-rw-r--r-- 1 analyst analyst      75 Mar 21  2018 elk_services
-rw-r--r-- 1 analyst analyst     373 Mar 21  2018 h2_dropbear.banner
drwxr-xr-x 2 analyst analyst    4096 Apr  2  2018 instructor
-rw-r--r-- 1 analyst analyst     255 Mar 21  2018 letter_to_grandma.txt
-rw-r--r-- 1 analyst analyst   24464 Mar 21  2018 logstash-tutorial.log
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 malware
-rwxr-xr-x 1 analyst analyst     172 Mar 21  2018 mininet_services
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 openssl_lab
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 pcaps
drwxr-xr-x 7 analyst analyst    4096 Mar 21  2018 pox
-rw-r--r-- 1 analyst analyst 473363 Mar 21  2018 sample.img
-rw-r--r-- 1 analyst analyst      65 Mar 21  2018 sample.img_SHA256.sig
drwxr-xr-x 3 analyst analyst    4096 Mar 21  2018 scripts
```

Log được tìm thấy trong tập tin **applicationX_in_epoch.log** thuộc máy ảo **CyberOps Workstation VM.**

Chuyển đổi Epoch thành dấu thời gian có thể đọc được với AWK. AWK là ngôn ngữ lập trình được thiết kế để thao tác với các tệp văn bản. Nó rất mạnh mẽ và đặc biệt hữu ích khi xử lý các tệp văn bản trong đó các dòng chứa nhiều trường, được phân tách bằng ký tự phân cách. Các tệp nhật ký chứa một mục nhập trên mỗi dòng và được định dạng dưới dạng các trường được phân

tách bằng dấu phân cách, làm cho AWK trở thành một công cụ tuyệt vời để chuẩn hóa.

Tệp nhật ký ở trên được tạo bởi ứng dụng X. Các khía cạnh liên quan của tệp là:

- Các cột được phân tách hoặc phân tách bằng dấu | thuộc tính. Do đó, tập tin có năm cột.

- Cột thứ ba chứa dấu thời gian trong Unix Epoch.

- Các tập tin có một dòng thêm vào cuối. Điều này sẽ quan trọng sau này trong khi thử nghiệm.

Dùng lệnh AWK để chuyển đổi và in kết quả ra màn hình:

awk 'BEGIN {FS=OFS="|"} {$3=strftime("%c",$3)} {print}' applicationX_in_epoch.log

```
[analyst@secOps lab.support.files]$ awk 'BEGIN {FS=OFS="|"}
{$3=strftime("%c",$3)} {print}' applicationX_in_epoch.log
2|Z|Mon 18 Aug 2008 11:00:00 AM EDT|AF|0
3|N|Tue 19 Aug 2008 11:00:00 AM EDT|AF|89
4|N|Sun 07 Sep 2008 11:00:00 AM EDT|AS|12
1|Z|Mon 08 Sep 2008 11:00:00 AM EDT|AS|67
5|N|Tue 09 Sep 2008 11:00:00 AM EDT|EU|23
6|R|Wed 10 Sep 2008 11:00:00 AM EDT|OC|89
||Wed 31 Dec 1969 07:00:00 PM EST
```

Dùng lệnh AWK để chuyển đổi log và ghi log và tập tin applicationX_in_hman.log

awk 'BEGIN {FS=OFS="|"} {$3=strftime("%c",$3)} {print}' applicationX_in_epoch.log > applicationX_in_human.log

```
[analyst@secOps lab.support.files]$ awk 'BEGIN {FS=OFS="|"}{$3=strftime("%c",$3)}
{print}' applicationX_in_epoch.log > applicationX_in_human.log
```

```
[analyst@secOps lab.support.files]$ cat applicationX_in_human.log
2|Z|Mon 18 Aug 2008 11:00:00 AM EDT|AF|0
3|N|Tue 19 Aug 2008 11:00:00 AM EDT|AF|89
4|N|Sun 07 Sep 2008 11:00:00 AM EDT|AS|12
1|Z|Mon 08 Sep 2008 11:00:00 AM EDT|AS|67
5|N|Tue 09 Sep 2008 11:00:00 AM EDT|EU|23
6|R|Wed 10 Sep 2008 11:00:00 AM EDT|OC|89
||Wed 31 Dec 1969 07:00:00 PM EST
```

Dùng lệnh AWK để chuyển đổi và in kết quả ra màn hình

```
[analyst@secOps lab.support.files]$ awk 'BEGIN {FS=
OFS=" "}{$4=strftime("%c",$4)} {print}' /home/analy
st/lab.support.files/apache_in_epoch.log
198.51.100.213 - - Wed 31 Dec 1969 07:00:00 PM EST
"GET /twiki/bin/edit/Main/Double_bounce_sender?topi
cparent=Main.ConfigurationVariables HTTP/1.1" 401 1
2846
198.51.100.213 - - Wed 31 Dec 1969 07:00:00 PM EST
"GET /twiki/bin/rdiff/TWiki/NewUserTemplate?rev1=1.
3&rev2=1.2 HTTP/1.1" 200 4523
```

```
198.51.100.213 - - Wed 31 Dec 1969 07:00:00 PM EST
"GET /mailman/listinfo/hsdivision HTTP/1.1" 200 629
1
198.51.100.213 - - Wed 31 Dec 1969 07:00:00 PM EST
"GET /twiki/bin/view/TWiki/WikiSyntax HTTP/1.1" 200
 7352
198.51.100.213 - - Wed 31 Dec 1969 07:00:00 PM EST
"GET /twiki/bin/view/Main/DCCAndPostFix HTTP/1.1" 2
00 5253
198.51.100.213 - - Wed 31 Dec 1969 07:00:00 PM EST
"GET /twiki/bin/oops/TWiki/AppendixFileSystem?templ
ate=oopsmore&m1=1.12&m2=1.12 HTTP/1.1" 200 11382
```

3.2. Kịch bản tấn công:

Máy tấn công (**Attacker)** thực hiện các mã lệnh tấn công vào máy chủ dữ liệu **Metaploit**.

Người quản trị tổ chức ngăn chặn tấn công tạm thời thông qua các công cụ hỗ trợ từ máy chủ CyberOps Worksation.

Sau khi hoàn tất quá trình ngăn chặn tấn công từ **Attacker**, người quản trị truy cập vào máy chủ nhật ký **Security Onion**.

Truy cập thành công vào máy chủ nhật ký, người quản trị sử dụng màn hình giám sát truy vấn các tập tin nhật ký từ máy chủ nhật ký.

Dùng các dữ liệu từ tập tin nhật ký để phân tích chi tiết cuộc tấn công. Từ việc phân tích trên, người quản trị sẽ có những giải pháp khắc phục và vá lỗ hổng.

3.3. ELSA log:

Dùng lệnh **cd** chuyển đường dẫn đến thư mục chứa tập tin nhật ký ELSA.

```
analyst@SecOnion:~/Desktop$ cd /nsm/elsa/data/elsa/log
analyst@SecOnion:/nsm/elsa/data/elsa/log$ ls -l
total 170096
-rw-rw---- 1 www-data sphinxsearch 57049170 Jun 18 08:06 node.log
-rw-rw---- 1 www-data sphinxsearch  6547557 Aug  3  2017 node.log.1.gz
-rw-rw---- 1 www-data sphinxsearch  7014600 Jul 17  2017 node.log.2.gz
-rw-rw---- 1 www-data sphinxsearch  6102122 Jul 13  2017 node.log.3.gz
-rw-rw---- 1 www-data sphinxsearch  4655874 Jul  8  2017 node.log.4.gz
-rw-rw---- 1 www-data sphinxsearch  6518229 Jun 18 08:06 query.log
-rw-rw---- 1 www-data sphinxsearch 53646286 Jun 18 08:06 searchd.log
-rw-rw---- 1 www-data sphinxsearch 32611837 Jun 18 08:06 web.log
```

3.4. Snort log:

Dùng lệnh **cd** chuyển đường dẫn đến thư mục chứa tập tin nhật ký Snort.

```
analyst@SecOnion:/nsm/sensor_data$ ls -l
total 16
drwxrwxr-x 7 sguil sguil 4096 Jun 19  2017 seconion-eth0
drwxrwxr-x 7 sguil sguil 4096 Jun 19  2017 seconion-eth1
drwxrwxr-x 7 sguil sguil 4096 Jun 19  2017 seconion-eth2
drwxrwxr-x 5 sguil sguil 4096 Jun 19  2017 seconion-eth3
```

```
analyst@SecOnion:/nsm/sensor_data$ ls -l seconion-eth0
total 144
drwxrwxr-x 2 sguil sguil   4096 Jun 19  2017 argus
drwxrwxr-x 5 sguil sguil   4096 Jun 18 08:04 dailylogs
drwxrwxr-x 2 sguil sguil   4096 Jun 19  2017 portscans
drwxrwxr-x 2 sguil sguil   4096 Jun 19  2017 sancp
drwxr-xr-x 2 sguil sguil   4096 Jun 18 08:16 snort-1
-rw-r--r-- 1 sguil sguil 121568 Jun 18 08:16 snort-1.stats
-rw-r--r-- 1 root  root       0 Jun 19  2017 snort.stats
```

3.5. Bro log:

Dùng lệnh **cd** chuyển đường dẫn đến thư mục chứa tập tin nhật ký Bro.

```
analyst@SecOnion:/nsm/bro/logs/current$ ls -l
total 124
-rw-rw-r-- 1 sguil sguil    368 Jun 18 08:21 capture_loss.log
-rw-rw-r-- 1 sguil sguil 61729 Jun 18 08:22 communication.log
-rw-rw-r-- 1 sguil sguil  3756 Jun 18 08:21 conn.log
-rw-rw-r-- 1 sguil sguil 25854 Jun 18 08:04 loaded_scripts.log
-rw-rw-r-- 1 sguil sguil   187 Jun 18 08:05 packet_filter.log
-rw-rw-r-- 1 sguil sguil  2683 Jun 18 08:06 reporter.log
-rw-rw-r-- 1 sguil sguil  1952 Jun 18 08:21 stats.log
-rw-rw-r-- 1 sguil sguil     0 Jun 18 08:04 stderr.log
-rw-rw-r-- 1 sguil sguil   188 Jun 18 08:04 stdout.log
-rw-rw-r-- 1 sguil sguil   933 Jun 18 08:06 weird.log
```

3.6. Various log:

Dùng lệnh **cd** chuyển đường dẫn đến thư mục chứa tập tin nhật ký Sguil.

```
analyst@SecOnion:/var/log/nsm$ ls -l
total 8364
-rw-r--r-- 1 sguil sguil          4 Jun 18 08:23 eth0-packets.log
-rw-r--r-- 1 sguil sguil          4 Jun 18 08:23 eth1-packets.log
-rw-r--r-- 1 sguil sguil          4 Jun 18 08:23 eth2-packets.log
-rw-r--r-- 1 sguil sguil        182 Jun 18 08:04 ossec_agent.log
-rw-r--r-- 1 sguil sguil        202 Jul 11  2017 ossec_agent.log.20170711120202
-rw-r--r-- 1 sguil sguil        202 Jul 13  2017 ossec_agent.log.20170713120201
-rw-r--r-- 1 sguil sguil        202 Jul 14  2017 ossec_agent.log.20170714120201
-rw-r--r-- 1 sguil sguil        202 Jul 15  2017 ossec_agent.log.20170715120202
-rw-r--r-- 1 sguil sguil        249 Jul 16  2017 ossec_agent.log.20170716120201
-rw-r--r-- 1 sguil sguil        202 Jul 17  2017 ossec_agent.log.20170717120202
-rw-r--r-- 1 sguil sguil        202 Jul 28  2017 ossec_agent.log.20170728120202
-rw-r--r-- 1 sguil sguil        202 Aug  2  2017 ossec_agent.log.20170802120201
-rw-r--r-- 1 sguil sguil        202 Aug  3  2017 ossec_agent.log.20170803120202
-rw-r--r-- 1 sguil sguil        202 Aug  4  2017 ossec_agent.log.20170804120201
-rw-r--r-- 1 sguil sguil      42002 Aug  4  2017 pulledpork.log
drwxr-xr-x 2 sguil sguil       4096 Jun 18 08:05 seconion-eth0
drwxr-xr-x 2 sguil sguil       4096 Jun 18 08:05 seconion-eth1
drwxr-xr-x 2 sguil sguil       4096 Jun 18 08:06 seconion-eth2
drwxr-xr-x 2 sguil sguil       4096 Jun 19  2017 securityonion
-rw-r--r-- 1 sguil sguil       1647 Jun 19  2017 securityonion-elsa-config.log
-rw-r--r-- 1 sguil sguil    7705626 Jun 18 08:33 sensor-clean.log
-rw-r--r-- 1 sguil sguil       1603 Aug  4  2017 sensor-newday-argus.log
-rw-r--r-- 1 sguil sguil       1603 Aug  4  2017 sensor-newday-http-agent.log
-rw-r--r-- 1 sguil sguil       8875 Aug  4  2017 sensor-newday-pcap.log
-rw-r--r-- 1 sguil sguil      53163 Aug  4  2017 sguil-db-purge.log
-rw-r--r-- 1 sguil sguil     369738 Aug  4  2017 sid_changes.log
-rw-r--r-- 1 sguil sguil      22598 Aug  8  2017 so-bro-cron.log
```

4. KẾT LUẬN

Bài toán giám sát an ninh mạng bằng phương pháp phân tích tệp tin nhật ký hệ thống là vấn đề cơ bản trong việc phân tích, xác định các truy cập trái phép từ bên ngoài cũng như nội tại của hệ thống mạng máy tính. Từ đó, quản trị viên hệ thống mạng máy tính của một cơ quan, doanh nghiệp sẻ đề ra các biện pháp phòng tránh và ngăn chặn các mối đe dọa đến sự vận hành ổn định của hệ thống. Đề tài đã đề xuất phương pháp giám sát an ninh mạng bằng việc phân tích tệp tin nhật ký hệ thống qua nhiều hình thức khác nhau. Bài toán này đặt ra một thách thức lớn đối với các hệ thống hiện tại trong việc nâng cao khả năng bảo mật, chống lại các cuộc tấn công từ các tin tặc. Hướng phát triển của đề tài là tiếp tục nâng cao sự tối ưu trong việc ghi nhận và khai thác dữ liệu từ tập tin nhật ký hệ thống, qua đó nâng cao hiệu quả trong việc giám sát./.

TÀI LIỆU THAM KHẢO

(1). Simson L.Garfinkel, Digital forensics research: The next 10 years, 2010.

(2). Paul SyversonGene TsudikMichael ReedCarl Landwehr, Towards an Analysis of Onion Routing Security, 2001.

(3). Lorraine F. BarrettWilliam C. Russell, Outputting a Network device Log file, 1995.

(4). Gideon FostickGil Bul, Voice session Data session interoperability in the Telephony environment, 2004.

(5). Edward W. Fordyce, IIIBarbara Elizabeth Patterson, Payment account processing which Conveys financial transaction data and non Financial transaction data, 2008.

(6). Jeffrey Heer, George Robertson, Animated Transitions in Statistical Data Graphics, 2007.

(7). B. Claise, Ed., Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information, 2008.

(8). BS Chaudhari, DRRS PRASAD, Particle Swarm Optimization Based Intrusion Detection for Mobile Ad-hoc Networks, 2015.

(9). TM Lin, CH Lee, JP Cheng, Prioritized random access with dynamic access barring for MTC in 3GPP LTE-A networks, 2014.

(10). G Vandenberghe - International Workshop on Visualization for Computer, Network traffic exploration application: A tool to assess, visualize, and analyze network security events, 2008.

(11). SA Edwards, The Programming Language Landscape, 2014.

(12). EM Daly, M Haahr, Social network analysis for routing in disconnected delay-tolerant manets, 2007.

(13). X Liu, X Zhang, D Yang - IEEE Communications Letters, Outage probability analysis of multiuser amplify-and-forward relay network with the source-to-destination links, 2011.