ĐẠI HỌC ĐÀ NẴNG

TRƯỜNG ĐẠI HỌC BÁCH KHOA

KHOA CÔNG NGHỆ THÔNG TIN

Tel. (+84.0236) 3736949, Fax. (84-511) 3842771

Website: http://dut.udn.vn/khoacntt, E-mail: cntt@dut.udn.vn

A blue and white logo with black text

Description automatically generated

BÁO CÁO THỰC TẬP TUẦN 4

THỰC TẬP TỐT NGHIỆP

Đề tài:

ULOGD

|  |  |  |
| --- | --- | --- |
| Họ và tên | Mã số sinh viên | Lớp học phần |
| Thân Nguyên Minh Quân | 102200148 | 20Nh14 |
| Hoàng Huân | 102200131 | 20Nh14 |
| Huỳnh Nguyễn Tấn Sang | 102200230 | 20Nh14 |

CBHD: TS Nguyễn Thế Xuân Ly

Đà Nẵng, 11/2024

MỤC LỤC

[**I.** **NỘI DUNG TUẦN 4** 3](#_Toc185839905)

[**II.** **TRIỂN KHAI CÁC YÊU CẦU** 4](#_Toc185839906)

[**1.** **Tìm hiểu các Plugin** 4](#_Toc185839907)

[**1.1.** **Input Plugin** 4](#_Toc185839908)

[**1.2.** **Output Plugin** 4](#_Toc185839909)

[**2.** **Xây dựng Ulogd tuỳ biến dựa vào các plugins** 5](#_Toc185839910)

[**2.1.** **Iptables** 5](#_Toc185839911)

[**2.2.** **NFLOG** 5](#_Toc185839912)

[**2.2.1.** **LOGEMU:** 5](#_Toc185839913)

[**2.2.2.** **Json & Xml** 6](#_Toc185839914)

[**2.2.3.** **PCAP** 8](#_Toc185839915)

[**2.2.4.** **Gprint** 9](#_Toc185839916)

[**2.2.5.** **OPRINT** 10](#_Toc185839917)

[**2.2.6.** **SQLITE3** 12](#_Toc185839918)

[**2.3.** **NFCT** 13](#_Toc185839919)

[**2.3.1.** **LOGEMU** 13](#_Toc185839920)

[**2.3.2.** **JSON, XML** 14](#_Toc185839921)

[**2.3.3.** **NACCT** 15](#_Toc185839922)

[**2.3.4.** **Oprint** 16](#_Toc185839923)

[**2.3.5.** **IPFIX** 18](#_Toc185839924)

[**2.4.** **Demo** 19](#_Toc185839925)

[**2.5.** **Nhận xét** 21](#_Toc185839926)

1. **NỘI DUNG TUẦN 4**

**Ulogd** là một trình nền báo cáo các vấn đề liên quan đến netfilter/iptables. Việc này bao gồm báo cáo vi phạm bảo mật và kiểm toán trên mỗi gói tin. Ulogd còn cho phép báo cáo bảo mật và kiểm toán 1 cách linh hoạt (do người dùng tuỳ chỉnh) trên mỗi luồng lưu lượng.

1. Tìm hiểu các plugins
   1. Input plugins: ULOG, NFLOG, NFCT
   2. Output plugins: LOGEMU, OPRINT, SYSLOG, MYSQL, PGSQL, SQLITE3, PCAP, IPFIX, NACCT, JSON
   3. Tìm hiểu những plugins hỗ trợ trên Ulogd trên WebOS hiện tại.
2. Xây dựng Ulogd tuỳ biến dựa vào các plugins

Xây dựng Ulogd tuỳ biến để báo cáo các vi phạm/ kiểm toán về gói tin/ luồng lưu lượng (tất nhiên cần xây dựng trước chính sách bảo mật --> iptables --> kiểm tra vi phạm/kiểm toán dựa vào Ulogd tuỳ biến).

1. **TRIỂN KHAI CÁC YÊU CẦU**
2. **Tìm hiểu các Plugin**
   1. **Input Plugin**

Các plugin đầu vào sẽ thu thập thông tin từ các gói tin mạng và gửi dữ liệu đến ulogd để xử lý.

+ NFLOG: Thu thập thông tin từ các gói tin được ghi lại bởi Netfilter (iptables).

+ NFCT: Thu thập thông tin từ các bảng kết nối Netfilter (connection tracking).

+ ULOG: Thu thập dữ liệu từ các gói tin được gửi qua các bộ lọc của Netfilter.

* 1. **Output Plugin**

Các plugin đầu ra định nghĩa cách thức lưu trữ hoặc hiển thị dữ liệu log. Một số plugin quan trọng:

+ LOGEMU: Ghi log theo kiểu log của kernel, giống với dmesg.

+ OPRINT: Xuất log ra màn hình terminal.

+ SYSLOG: Ghi log vào hệ thống log của Linux, thường nằm ở /var/log/syslog.

+ MYSQL, PGSQL, SQLITE3: Lưu log vào cơ sở dữ liệu tương ứng (MySQL, PostgreSQL, SQLite).

+ PCAP: Lưu gói tin ở định dạng PCAP, cho phép phân tích bằng các công cụ như Wireshark.

+ IPFIX: Lưu log theo chuẩn IP Flow Information Export, dùng cho giám sát lưu lượng mạng.

+ NACCT (Network Accounting): Theo dõi và lưu thông tin về lượng dữ liệu mạng truyền qua.

+ JSON: Lưu log dưới dạng JSON, dễ đọc và tích hợp vào các hệ thống phân tích hiện đại.

1. **Xây dựng Ulogd tuỳ biến dựa vào các plugins**
   1. **Iptables**

Xây dựng Rules Iptables ghi lại (logging) các gói tin vào log của hệ thống:

iptables -A INPUT -p icmp -m limit --limit 1/s --limit-burst 1 -j NFLOG --nflog-prefix "ping!!!" --nflog-group 1

* Rule này ghi lại các gói ICMP (ping) đến hệ thống, với tốc độ giới hạn là 1 gói mỗi giây, và prefix"ping!!!" sẽ được thêm vào log.

iptables -A INPUT -p tcp -m limit --limit 1/s --limit-burst 1 -j NFLOG --prefix "tcp!!!" --nflog-group 1

* Rule này ghi lại các gói TCP đến hệ thống, với tốc độ giới hạn là 1 gói mỗi giây, và prefix"tcp!!!" sẽ được thêm vào log.

Log nhóm chọn là Log2 và khai báo group=1

* 1. **NFLOG**
     1. **LOGEMU**

Logemu ghi lại các gói tin mạng dưới dạng văn bản

**Stack:** stack=log2:NFLOG,base1:BASE,ifi1:IFINDEX,ip2str1:IP2STR,print1:PRINTPKT,emu1:LOGEMU

**Cấu hình:**

BASE: Lưu trữ thông tin cơ bản của gói tin.

IFINDEX: Lấy chỉ số giao diện mạng.

IP2STR: Chuyển đổi địa chỉ IP thành dạng chuỗi dễ đọc.

PRINTPKT: In thông tin chi tiết của gói tin.

Log2:

A screenshot of a computer program

Description automatically generated

[emu1]

A white text on a purple background

Description automatically generatedS

**Kết quả:**

Register

****

Log

**A screen shot of a computer screen

Description automatically generated**

* + 1. **Json & Xml**

**Cấu hình:**

**A black background with white text

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**Kết quả:**

**A screen shot of a computer

Description automatically generated**

**A screen shot of a computer screen

Description automatically generated**

**A close up of a screen

Description automatically generated**

* + 1. **PCAP**

Ulogd lưu trữ các gói tin mạng được ghi lại dưới dạng tệp PCAP để phân tích bằng các công cụ như Wireshark.

**Stack:**

stack=log2:NFLOG,base1:BASE,pcap1:PCAP

**Cấu hình:**

**A computer screen shot of white text

Description automatically generated**

**Kết quả:**

**A screenshot of a computer program

Description automatically generated**

+ Đọc gói tin bằng tcpdump

A black and white screen

Description automatically generated

* + 1. **Gprint**

In ra thông tin gói tin mạng dưới dạng văn bản (plaintext) theo định dạng tùy chỉnh, giúp dễ dàng theo dõi và phân tích.

**Stack**: stack=log2:NFLOG,base1:BASE,gp1:GPRINT

**Cấu hình**:

A computer screen shot of a computer code

Description automatically generated

**Kết quả**:

A screenshot of a computer program

Description automatically generated

A screen shot of a computer screen

Description automatically generated

* + 1. **OPRINT**

In thông tin gói tin mạng ra đầu ra chuẩn (stdout) hoặc các hệ thống log khác theo định dạng cấu hình.

Stack: stack=log2:NFLOG,base1:BASE,ifi1:IFINDEX,ip2str1:IP2STR,print1:PRINTPKT,op1:OPRINT

Cấu hình:

A black background with white text

Description automatically generated

Kết quả:

A computer screen shot of white text

Description automatically generated

A screen shot of a computer

Description automatically generated

* + 1. **SQLITE3**

Lưu vào Database và truy vấn để xem thông tin log

**Stack:** stack=log20:NFLOG,base1:BASE,ifi1:IFINDEX,ip2str1:IP2STR,mac2str1:HWHDR,boot\_sqlt:SQLITE3

**Cấu hình:**

Log20: Group20

[boot\_sqlt]  
    table="all\_in"  
    db="/var/log/ulog/bootlog-sqlt3.db"

Tạo bảng all\_in bằng lệnh SQL với các trường là các thông tin của gói tin.

**Kết quả:**

A computer screen shot of a computer

Description automatically generated

Truy vấn bằng lệnh: SELECT \* FROM all\_in LIMIT 10;

A close up of a screen

Description automatically generated

Kết quả hiển thị các log, các gói tin icmp vượt đúng mức1/s thì sẽ bị đưa vào log cùng với prefix”ping”.

* 1. **NFCT**

NFCT trong ulogd bắt và ghi lại các thông tin về trạng thái kết nối (connection tracking) của các gói tin mạng, giúp theo dõi và phân tích các kết nối mạng.

* + 1. **LOGEMU**

**Stack:**

stack=ct1:NFCT,ip2str1:IP2STR,print1:PRINTFLOW,emu1:LOGEMU

**Cấu hình:**

**A screen shot of a computer

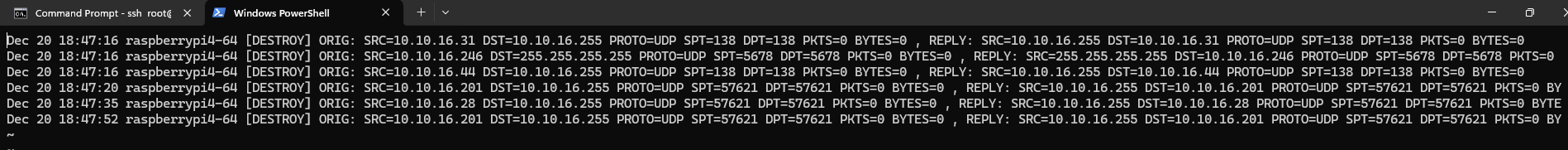
Description automatically generated**

**Kết quả:**

**A screenshot of a computer

Description automatically generated**

**[Log]**

****

* + 1. **JSON, XML**

**Stack:**

stack=ct1:NFCT,json1:JSON

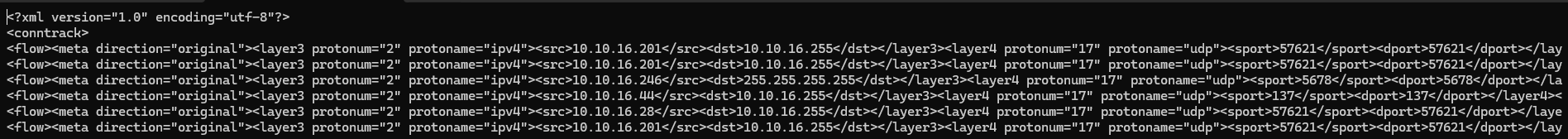
stack=ct1:NFCT,xml1:XML

**Kết quả:**

A screenshot of a computer program

Description automatically generated

**[Log]**

****

A screenshot of a computer

Description automatically generated

**[Log]**

**A screen shot of a computer screen

Description automatically generated**

* + 1. **NACCT**

nacct là một module được sử dụng để tính toán số lượng các gói dữ liệu trong một khoảng thời gian nhất định

**Stack:**

stack=ct1:NFCT,ip2str1:IP2STR,nacct1:NACCT

**Kết quả:**

**A screenshot of a computer

Description automatically generated**

Thông tin về các gói dữ liệu, bao gồm các thông tin như số lượng gói, số lượng byte, và thông tin khác liên quan đến mạng.

**A screenshot of a computer

Description automatically generated**

* + 1. **Oprint**

**Stack:**

stack=ct1:NFCT,op1:OPRINT

**Cấu hình:**

**A black background with white text

Description automatically generated**

**Kết quả:**

**A screenshot of a computer

Description automatically generated**

**A screen shot of a computer program

Description automatically generated**

* + 1. **IPFIX**

Cho biết các thông tin về lưu lượng mạng (như địa chỉ IP nguồn, đích, cổng, số lượng byte/gói)

**Stack:**

stack=ct1:NFCT,iffix1:IPFIX

**Cấu hình:**

Ở máy đích bật netcat lắng nghe và bắt gói tin bằng wireshark

**A screenshot of a computer program

Description automatically generated**

**Kết quả:**

**A screen shot of a computer

Description automatically generated**

**A screenshot of a computer screen

Description automatically generated**

Nhưng không đọc được nội dung gói tin

**A screenshot of a computer

Description automatically generated**

* 1. **Demo**

**Đầu vào:**

- Giả sử đã tuỳ chỉnh file ulogd.conf.in.user:

- Input plugin: NFLOG

- Output: JSON and LOGEMU

**Đầu ra:***Gồm 2 file full.log và firewall\_log.json*

**iptables:** Thiết lập 2 Rules vào hệ thống

**A black background with white text

Description automatically generated**

**Stack:**

**A screen shot of a computer

Description automatically generated**

**Kết quả:**

**A screen shot of a computer

Description automatically generated**

**Log:**

**A black screen with white text

Description automatically generated**

**[Logemu]**

**A screen shot of a computer

Description automatically generated**

**[Json]**

**A screenshot of a computer

Description automatically generated**

* 1. **Nhận xét**

Nhóm đã triển khai Ulogd thành công với Input: Nflog và NFCT, Output: Logemu, Json Xml, PCAP, NACCT, Oprint, Gprint, SQLITE3, IPFIX... Các kết quả cho thấy đã trích xuất log thành công, với Nflog là tùy biến theo Iptables và Nfct theo dõi các kết nối mạng.

|  |  |  |
| --- | --- | --- |
| **Output\Input** | **NFLOG** | **NFCT** |
| **LOGEMU** | x | x |
| **JSON, XML** | x | xS |
| **PCAP** | x |  |
| **SYSLOG** |  |  |
| **IPFIX** |  | x |
| **NACCT** |  | x |
| **OPRINT** | x | x |
| **GPRINT** | x |  |
| **SQLITE3** | x |  |
| **MYSQL, PostgreSQL** |  |  |