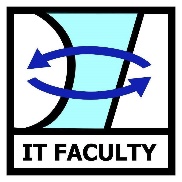
ĐẠI HỌC ĐÀ NẴNG

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



BÁO CÁO THỰC TẬP TUẦN 6

THỰC TẬP TỐT NGHIỆP

Đề tài:

Nflog API

|  |  |  |
| --- | --- | --- |
| 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

Đà Nẵng, 12/2024

MỤC LỤC

[I. Nội dung tuần 6 3](#_Toc187055765)

[**1. Nội dung 3**](#_Toc187055766)

[**1.1. Sequence Diagram 3**](#_Toc187055767)

[**2. Yêu cầu triển khai: 3**](#_Toc187055768)

[**2.1. Dựa vào Sequence Diagram hãy xây dựng API của Nflog để thu thập và báo cáo các thao tác của người dùng khi tương tác với WebOS trên Raspberry. 3**](#_Toc187055769)

[**2.2. Chỉ ra các vi phạm vào chính sách tường lửa của người dùng. 3**](#_Toc187055770)

[II. Triển khai các yêu cầu 4](#_Toc187055771)

[**1.** **Ulogd** 4](#_Toc187055772)

[**2.** **Iptables** 5](#_Toc187055773)

[**3.** **Nflog API** 5](#_Toc187055774)

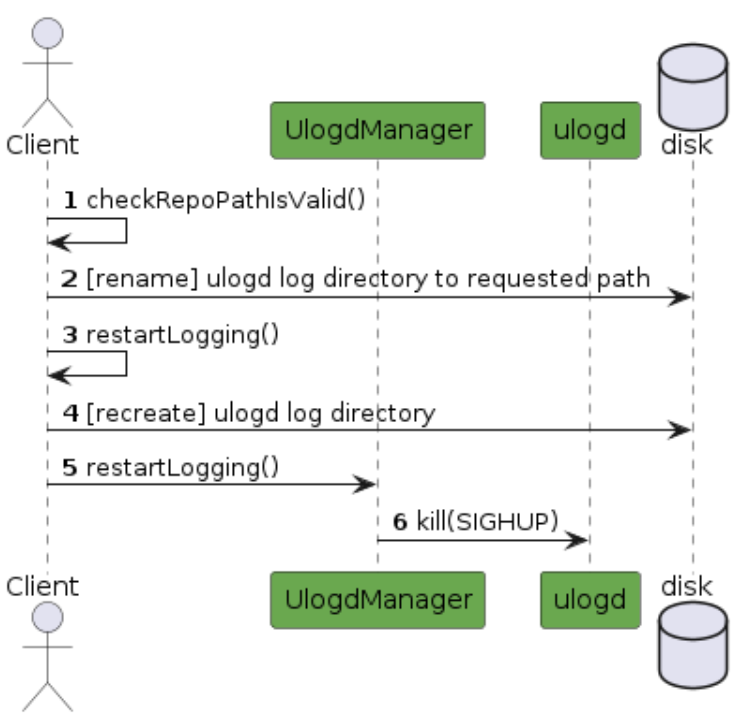
[**4.** **Demo** 8](#_Toc187055775)

[**5.** **Kết Luận:** 12](#_Toc187055776)

1. Nội dung tuần 6

1. Nội dung

1.1. Sequence Diagram



2. Yêu cầu triển khai:

2.1. Dựa vào Sequence Diagram hãy xây dựng API của Nflog để thu thập và báo cáo các thao tác của người dùng khi tương tác với WebOS trên Raspberry.

2.2. Chỉ ra các vi phạm vào chính sách tường lửa của người dùng.

1. Triển khai các yêu cầu
2. **Ulogd**

Cài đặt stack phù hợp cho Ulogd, tạo các group và các log file tương ứng với các group.

stack=log25:NFLOG,base1:BASE,ifi1:IFINDEX,ip2str1:IP2STR,print1:PRINTPKT,emu1:LOGEMU

stack=log20:NFLOG,base1:BASE,xml1:XML

stack=log21:NFLOG,base1:BASE,ifi1:IFINDEX,ip2str1:IP2STR,mac2str1:HWHDR,json1:JSON

stack=log22:NFLOG,base1:BASE,pcap1:PCAP

stack=log23:NFLOG,base1:BASE,gp1:GPRINT

stack=log24:NFLOG,base1:BASE,ifi1:IFINDEX,ip2str1:IP2STR,print1:PRINTPKT,op1:OPRINT

[log25]  
 group=25

[log20]  
 group=20

[log21]  
 group=21

[log22]  
 group=22

[log23]  
 group=23

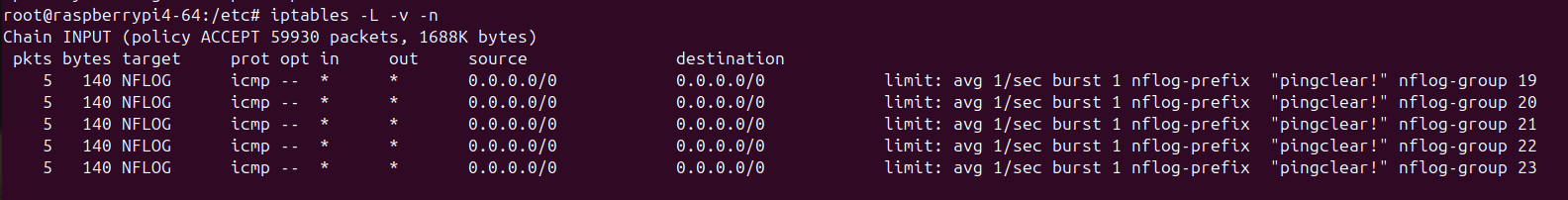
[log24]  
 group=24

1. **Iptables**

Tạo Rules Iptables để nhận log cảnh báo

iptables -A INPUT -p icmp -m limit --limit 1/s --limit-burst 1 -j NFLOG --nflog-prefix "pingclear!" --nflog-group 19

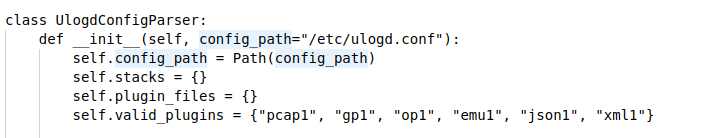
Tương ứng tiếp cho các group19->23. Ở đây lấy chung Protocol để kiểm tra tiện hơn.



1. **Nflog API**

Đầu tiên nhóm sẽ detect ra được những cái stack sử dụng trong trong ulogd.conf.

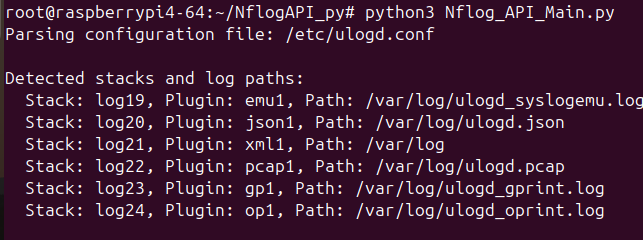
Dùng Python để phân tích cấu hình của ulogd, thu thập và hiển thị các log từ các plugin khác nhau (như PCAP, JSON, syslogEMU, v.v.).



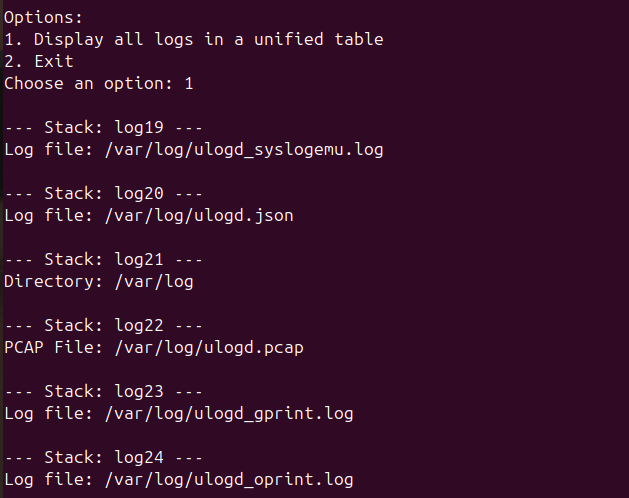
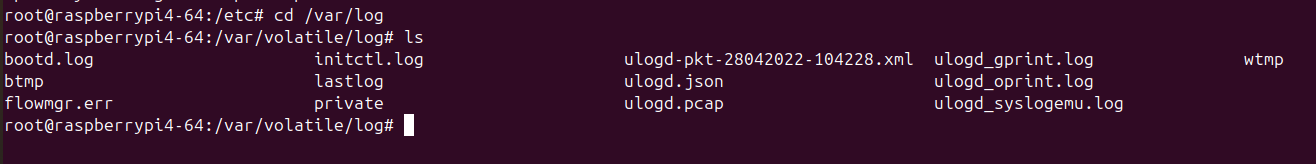
Ở đây set cứng các tham số plugin như pcap1, emu1...

* Kiểm tra sự tồn tại của file cấu hình (/etc/ulogd.conf).
* Đọc từng dòng trong file cấu hình và xử lý:
* Nếu dòng bắt đầu với stack=, tìm kiếm tên của stack và các plugin kèm theo.
* Nếu có file= hoặc directory=, tìm kiếm đường dẫn của các file log hoặc thư mục.

Code detect ra các plugin và nhóm log trong file conf được sử dụng.



Sau đó có tùy chọn trích dẫn đường dẫn các file đã tìm thấy trong cấu hình:



* **Phương thức display\_logs**:

Kiểm tra xem có logs hay không.

Duyệt qua các stack và plugin, xác định xem log có ở dạng file hay thư mục.

Gọi các phương thức phù hợp để thu thập log từ file, thư mục hoặc PCAP.

Cuối cùng, hiển thị các log dưới dạng bảng.

* **Các phương thức thu thập log từ file hoặc thư mục**:

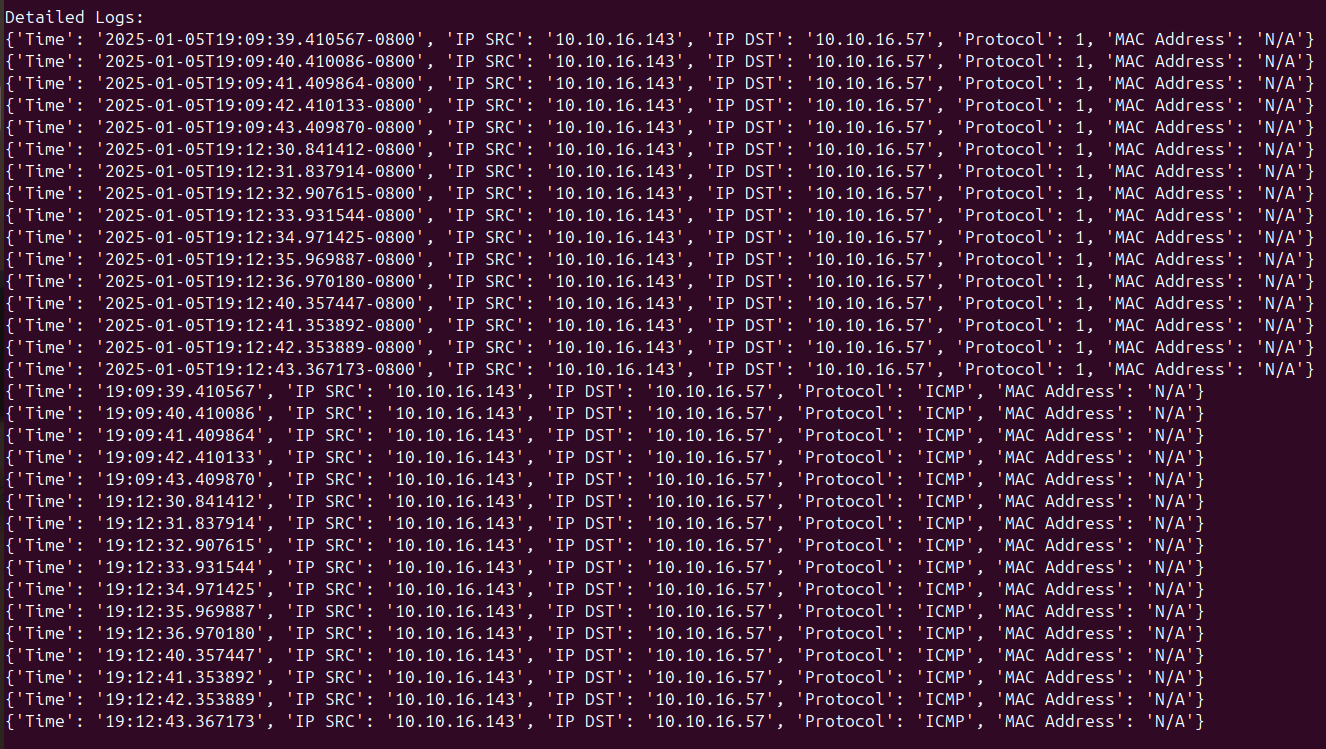
**collect\_log\_file**: Đọc log từ một file đơn lẻ và xử lý dựa trên loại plugin.

**collect\_directory\_logs**: Duyệt qua tất cả các file trong thư mục có phần mở rộng phù hợp với plugin (ví dụ: .json, .xml).

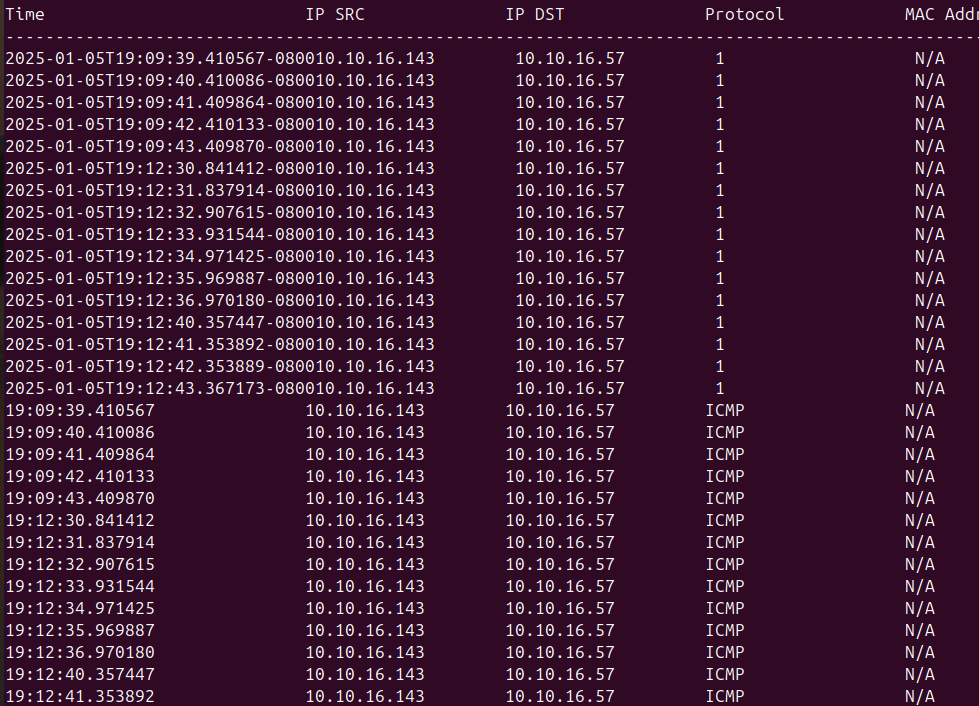
**collect\_pcap\_file**: Dùng tcpdump để đọc và phân tích một file PCAP.

List các file log ra dưới dạng DataFrame:

Triển khai dưới dạng DataFrame bằng Pandas Python:



Hoặc có thể là dạng bảng:

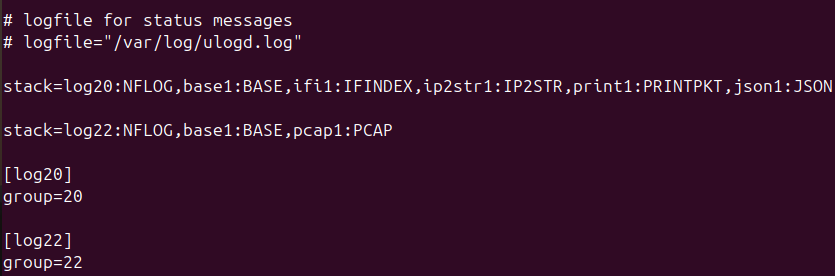


Khi có log file mới được cập nhật vào file config, khởi động lại chương trình để có thể đọc được cái plugin đăng kí trong ulogd.conf. Và không có yêu cầu RealTime.

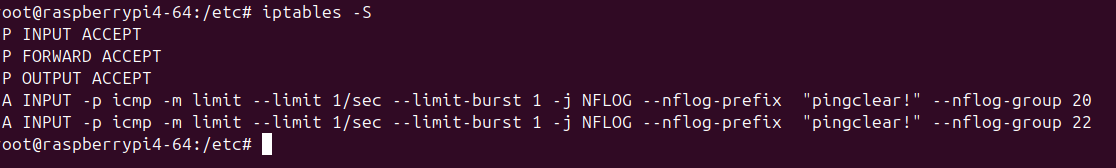
1. **Demo**

Nhóm sẽ dùng 2 plugin là Pcap và Json để để thu thập log

Cấu hình trong ulogd:

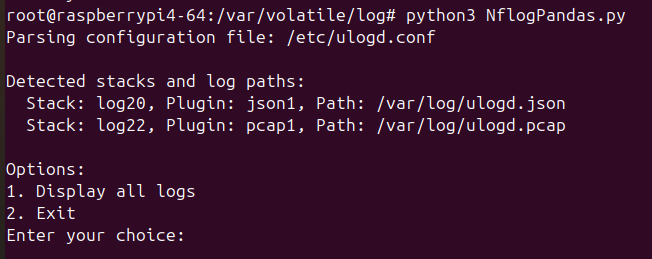


Cấu hình Rules tương tự trong Iptables để thu thập log về 2 group20-22



**Detect Stack và Check Valid Repo:**

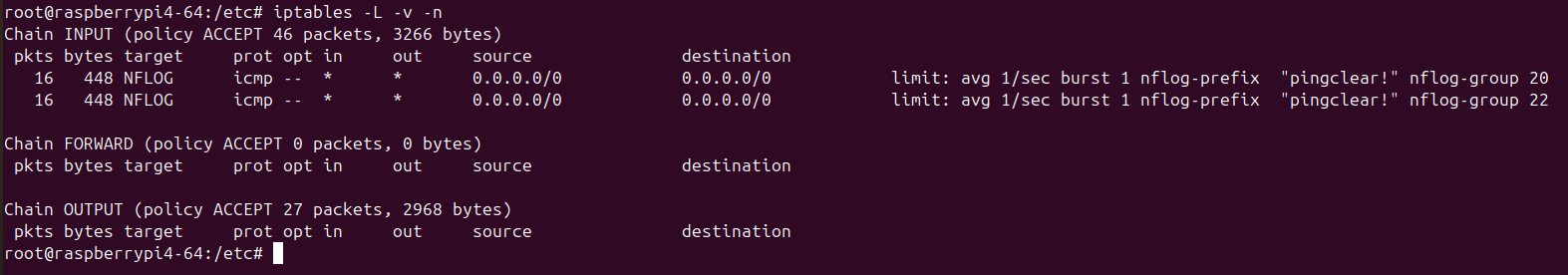
Code detect ra 2 stack sử dụng trong bài, cũng như là đường dẫn file chính xác.



Dùng Hping3 để tạo log trong iptables

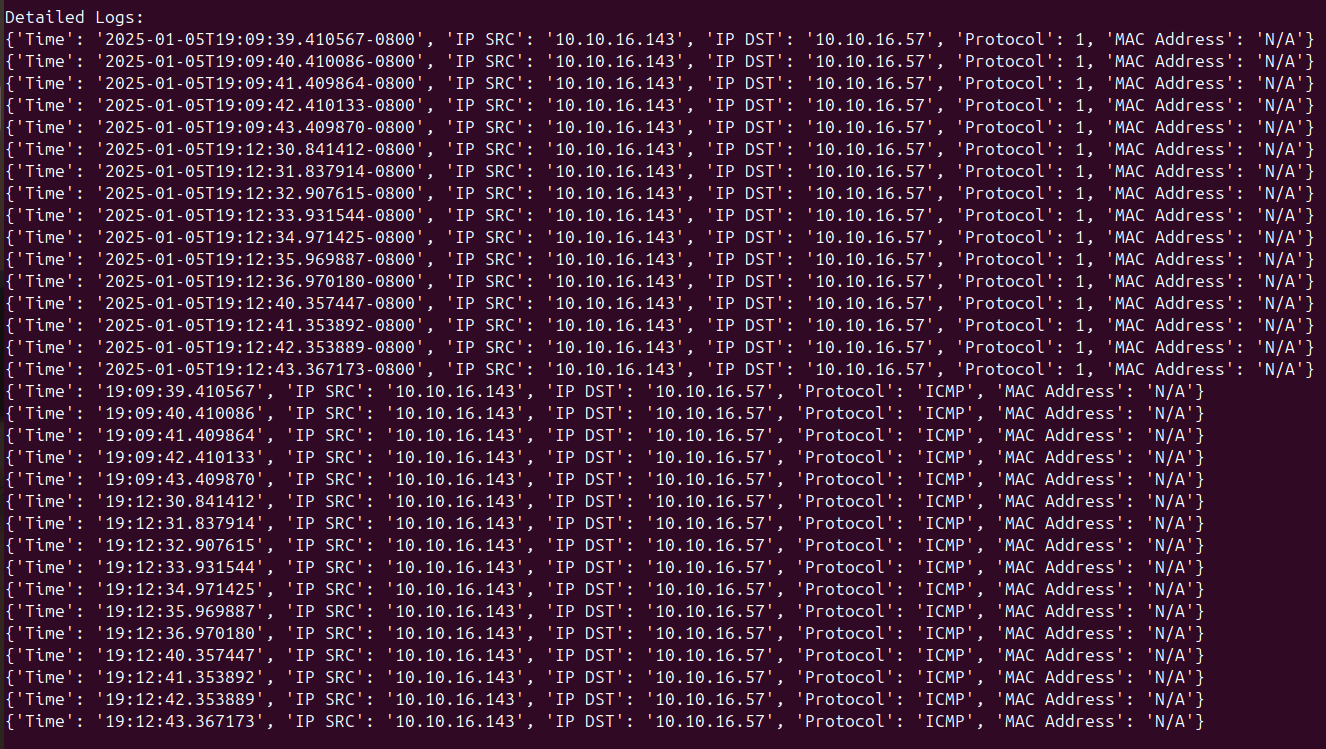
Hping3 –icmp --flood 10.10.16.57

Sau khi kiểm tra Iptables nhận thấy có các thông số về log được lưu:

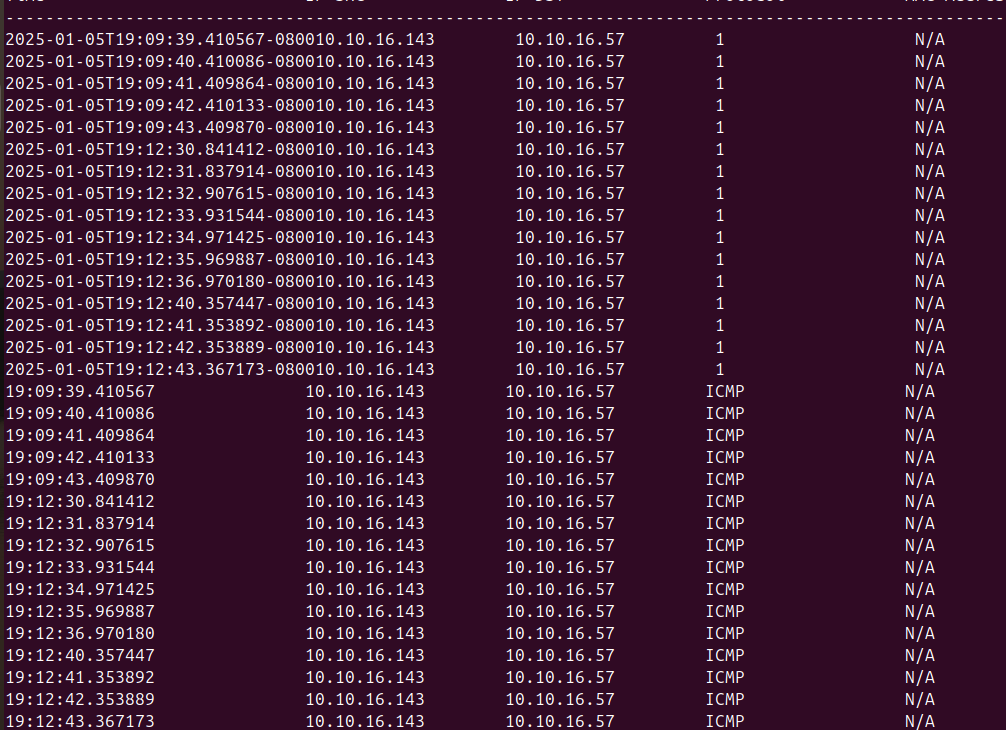


List Log:  
Dạng DataFrame

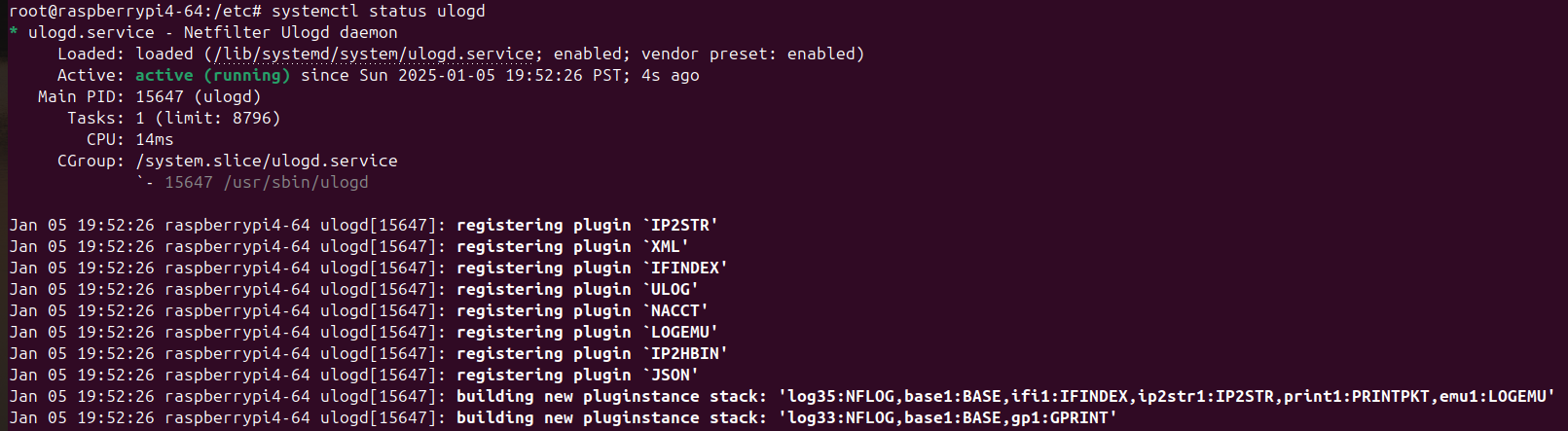
Không có thông tin về MAC nên sẽ hiển thị là N/A



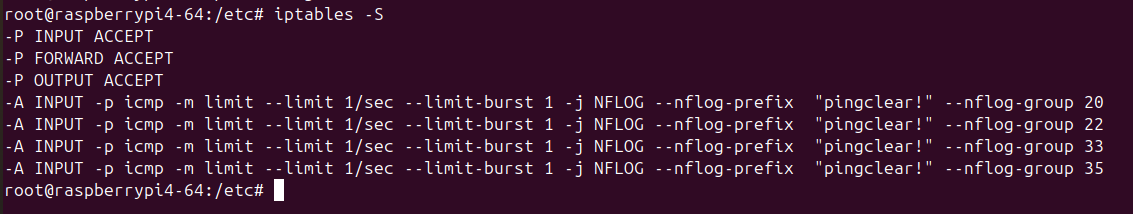
Hoặc có thể list ra dạng bảng :



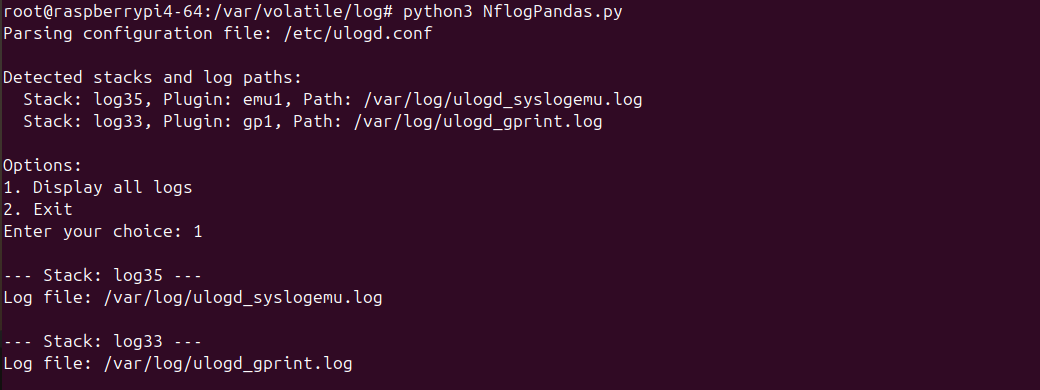
Tiếp theo, Nhóm sẽ làm 2 kiểu Logemu, Gprint



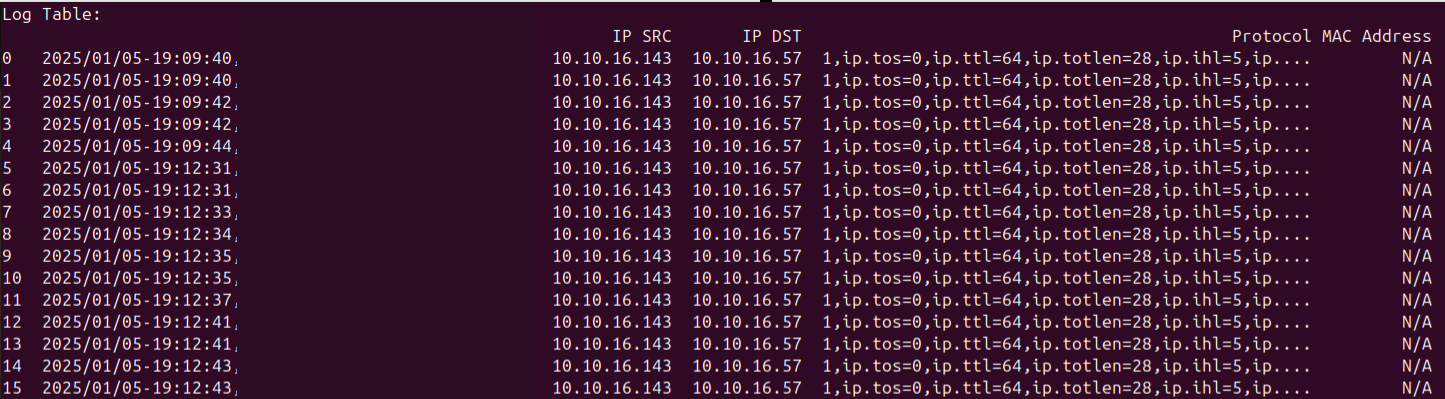
Thêm 2 rules mới vào để log về group



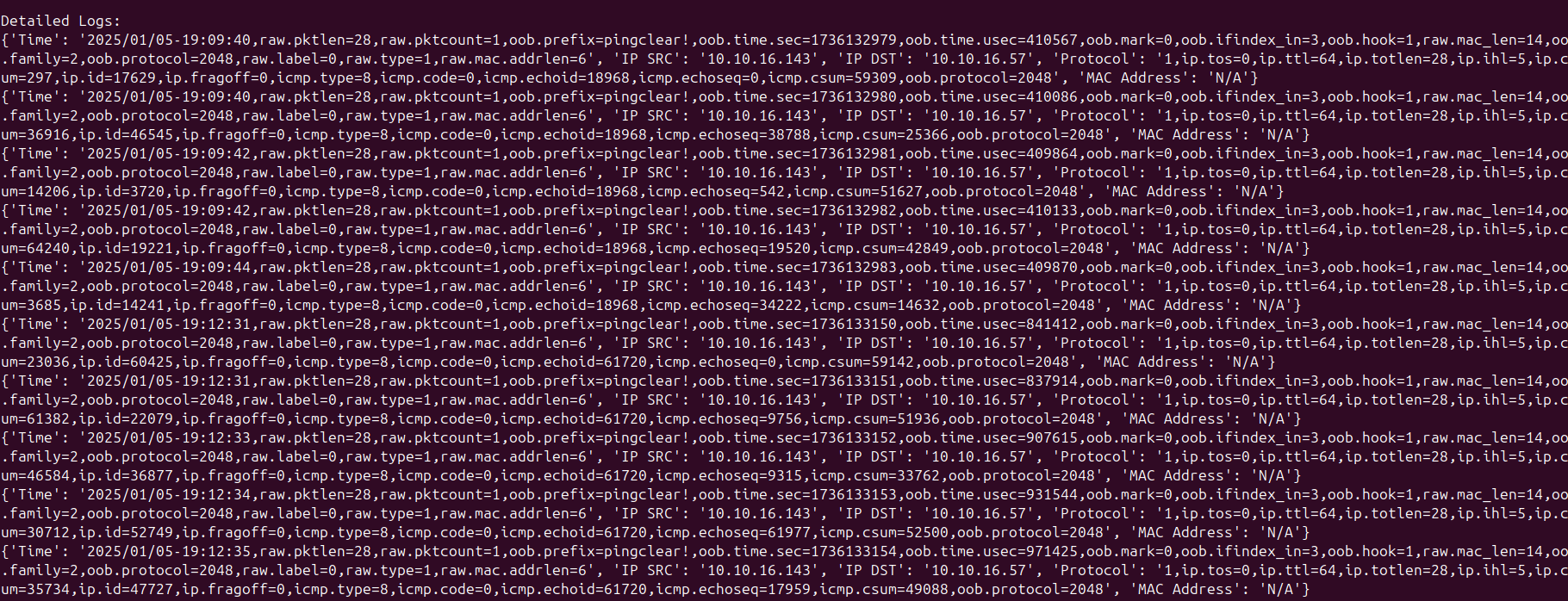
**Detect Stack và Check Valid Repo:**



List logemu ra dạng bảng:



List log detail cho Gprint vì Gprint chứa khá nhiều thông tin.



1. **Kết Luận:**

* Nhóm đã triển khai các bước để thu thập log trong Ulogd, các stack được cấu hình đúng, đã thu thập được log và hiển thị trong file.
* Xây dựng code detect tự động và list file ra các định dạng khác nhau tùy với cơ chế của loại file đó.
* Các kết quả cho thấy code hoạt động tốt và detect cũng như kiểm tra link file hợp lệ, đầu ra cho kết quả trực quan và rõ ràng.