

# Quản Trị Mạng Sử Dụng Raspberry Pi

Trần Anh Toàn  
Trịnh Minh Việt  
Trần Lê Long Vũ

GVHD: TS. Trần Thị Minh Hạnh

Khoa Điện tử – Viễn thông  
Trường Đại học Bách khoa – Đại học Đà Nẵng

Tháng 12/2025

# Mục lục

- 1 Giới thiệu
- 2 Mục tiêu đề tài
- 3 Phần cứng và thiết kế
- 4 Phương pháp thực hiện
- 5 Kết quả thực nghiệm
- 6 Kết luận
- 7 Tài liệu tham khảo

# Mục lục

- 1 Giới thiệu
- 2 Mục tiêu đề tài
- 3 Phần cứng và thiết kế
- 4 Phương pháp thực hiện
- 5 Kết quả thực nghiệm
- 6 Kết luận
- 7 Tài liệu tham khảo

# Giới thiệu

## Tình hình hiện nay:

- Các công cụ giám sát mạng truyền thống chi phí cao
- Phụ thuộc vào phần cứng chuyên dụng đắt tiền
- Thiếu khả năng quan sát toàn bộ luồng dữ liệu trong mạng
- Khó triển khai cho mạng quy mô nhỏ và vừa

## Đề tài này khắc phục:

- Giải pháp chi phí thấp dựa trên Raspberry Pi
- Tích hợp đầy đủ: thu thập - phân tích - hiển thị - kiểm soát
- Quan sát toàn bộ lưu lượng qua kiến trúc bridge
- Chủ động phát hiện và chặn tấn công
- Dễ dàng triển khai, phù hợp mạng nhỏ và vừa

# Mục lục

- 1 Giới thiệu
- 2 Mục tiêu đề tài
- 3 Phần cứng và thiết kế
- 4 Phương pháp thực hiện
- 5 Kết quả thực nghiệm
- 6 Kết luận
- 7 Tài liệu tham khảo

# Mục tiêu đề tài

## Thu thập và hiển thị:

- Lưu lượng truyền tải
- Độ trễ phản hồi
- Tỉ lệ mất gói
- Phân bố giao thức
- Dashboard web trực quan

## Chức năng bảo mật:

- Chặn IP nguy hiểm

# Mục lục

- 1 Giới thiệu
- 2 Mục tiêu đề tài
- 3 Phần cứng và thiết kế
- 4 Phương pháp thực hiện
- 5 Kết quả thực nghiệm
- 6 Kết luận
- 7 Tài liệu tham khảo

# Phần cứng sử dụng



Raspberry Pi 4



USB to LAN



Dây LAN

## Các dụng cụ chính

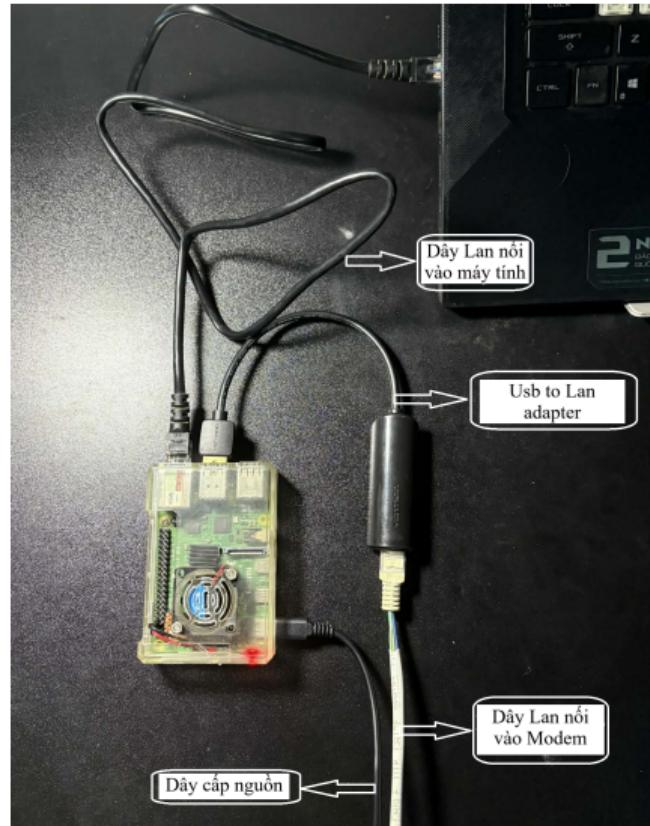
# Topology hệ thống

## Cấu trúc:

- Man-in-the-Middle
- Pi giữa máy chủ và modem
- Remote qua máy tính A

## Lợi ích:

- Theo dõi toàn bộ
- Giám sát chuyên dụng



Topology chính

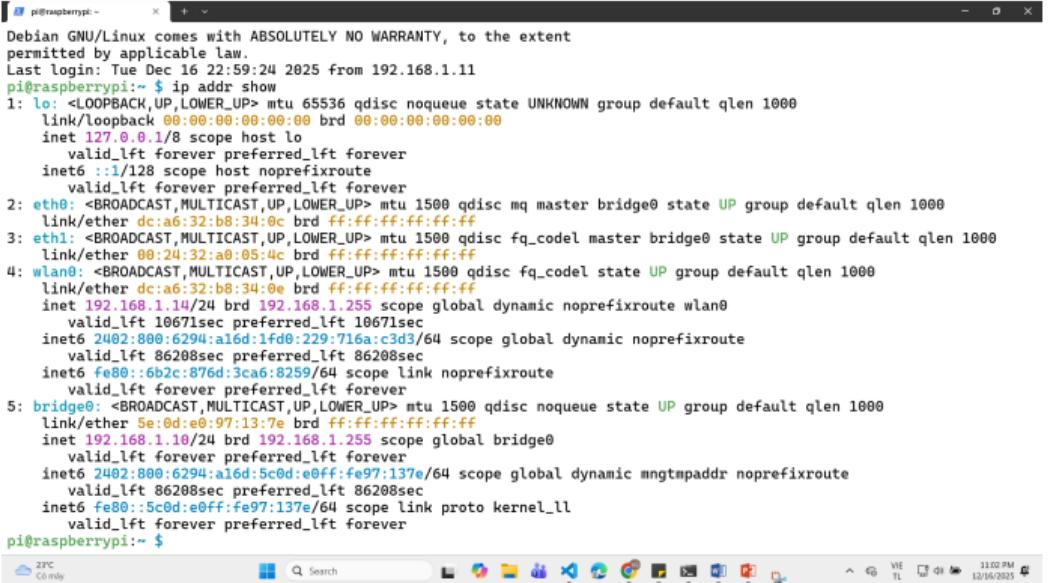
# Cấu hình Bridge thành công

## Xác nhận:

- Giao diện bridge0: UP
- eth0 và eth1 được gán vào bridge0

## Ý nghĩa:

- Raspberry Pi đóng vai trò bridge
- Có thể giám sát toàn bộ lưu lượng
- Network Monitor hiệu quả



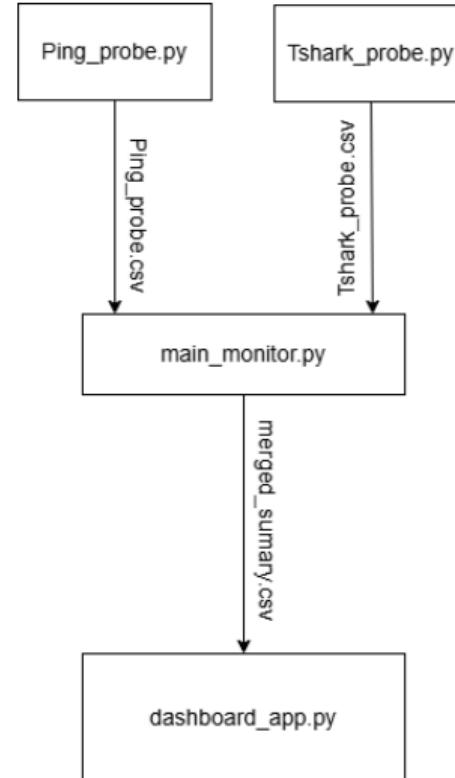
```
pi@raspberrypi: ~
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Dec 16 22:59:24 2025 from 192.168.1.11
pi@raspberrypi: ~ $ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master bridge0 state UP group default qlen 1000
    link/ether dc:a6:32:b8:34:0c brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel master bridge0 state UP group default qlen 1000
    link/ether 00:24:32:a0:05:4c brd ff:ff:ff:ff:ff:ff
4: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether dc:a6:32:b8:34:0e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.14/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
        valid_lft 10671sec preferred_lft 10671sec
        inet6 2402:800:6294:a16d:1fd0:229:716a:c3d/64 scope global dynamic noprefixroute
            valid_lft 86208sec preferred_lft 86208sec
        inet6 fe80::6b2c:876d:3ca6:8259/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
5: bridge0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 5e:0d:e0:97:13:7e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global bridge0
        valid_lft forever preferred_lft forever
        inet6 2402:800:6294:a16d:5c0d:e0ff:fe97:137e/64 scope global dynamic mngtmpaddr noprefixroute
            valid_lft 86208sec preferred_lft 86208sec
        inet6 fe80::5c0d:e0ff:fe97:137e/64 scope link proto kernel_ll
            valid_lft forever preferred_lft forever
pi@raspberrypi: ~ $
```

Kết quả lệnh ip addr show

# Mục lục

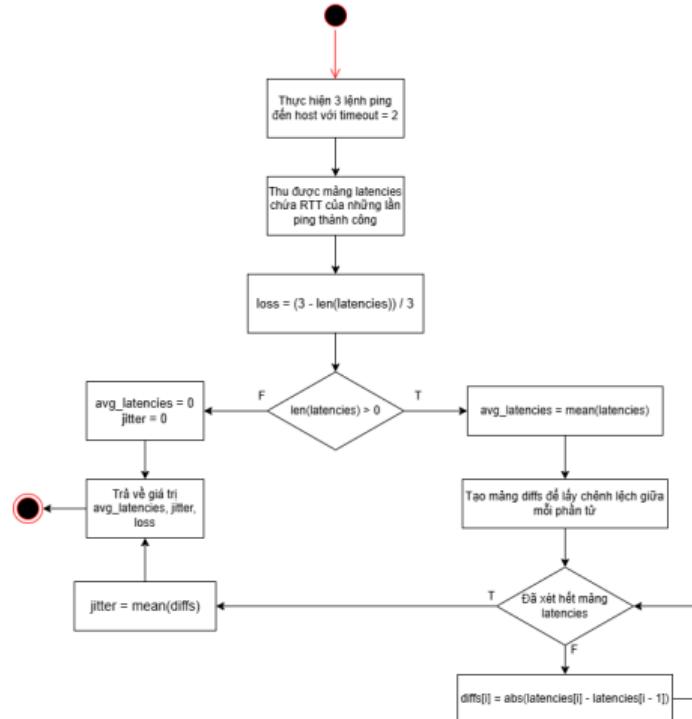
- 1 Giới thiệu
- 2 Mục tiêu đề tài
- 3 Phần cứng và thiết kế
- 4 Phương pháp thực hiện
- 5 Kết quả thực nghiệm
- 6 Kết luận
- 7 Tài liệu tham khảo

# Kiến trúc hệ thống giám sát

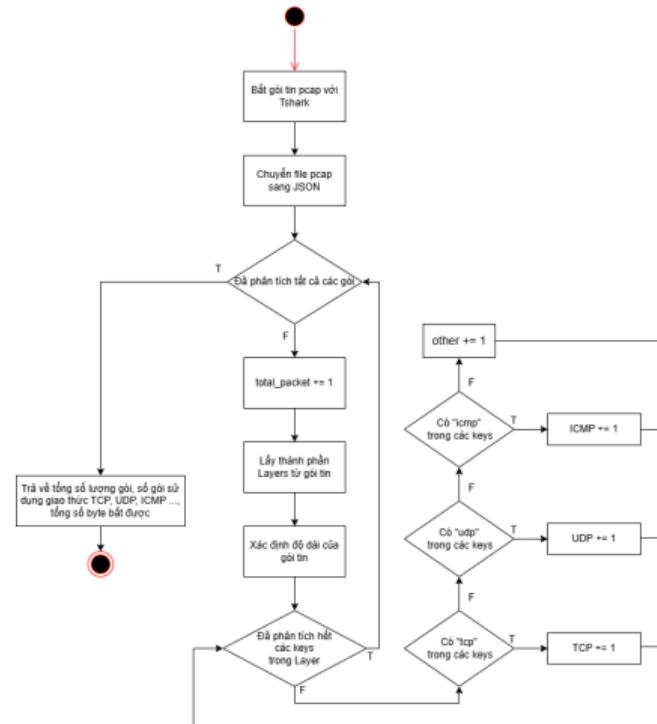


Sơ đồ khái hệ thống

# Module giám sát

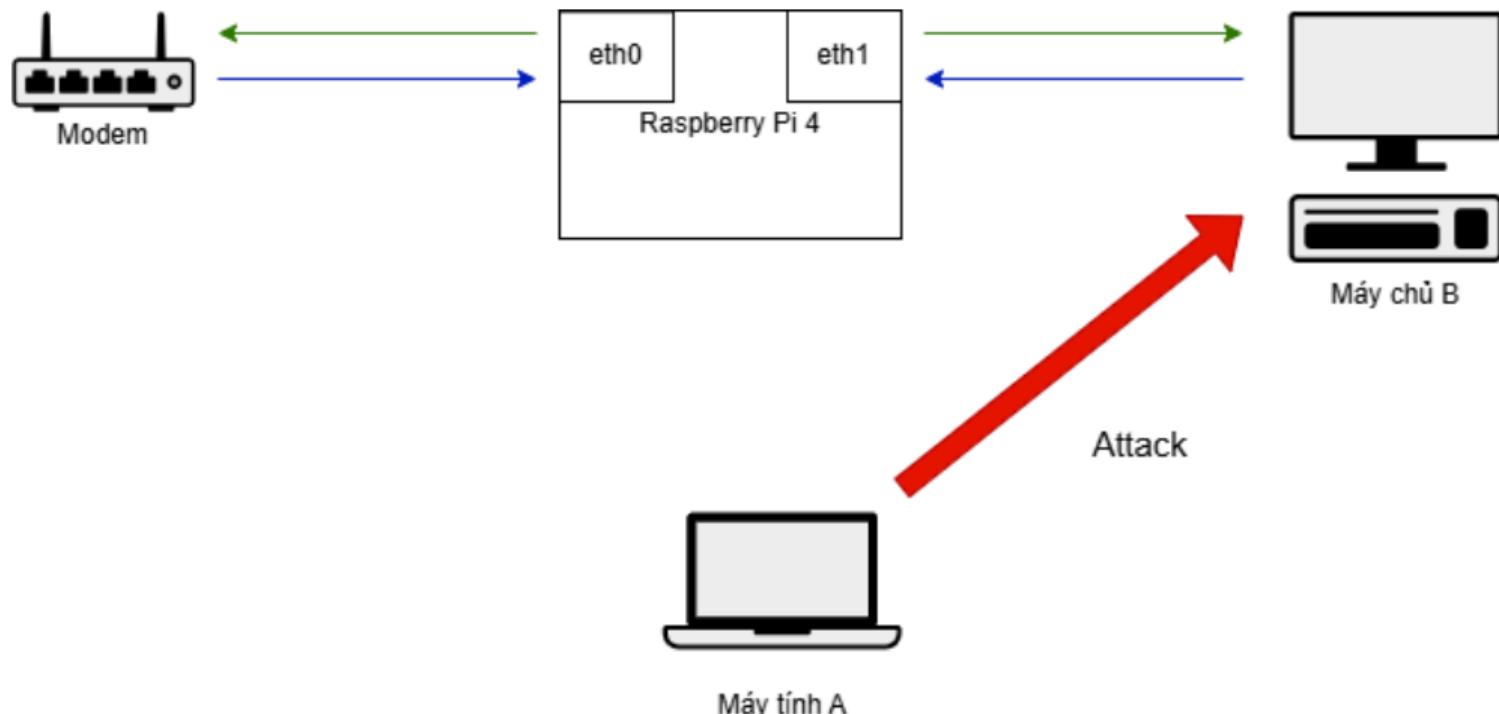


Lưu đồ Ping Probe



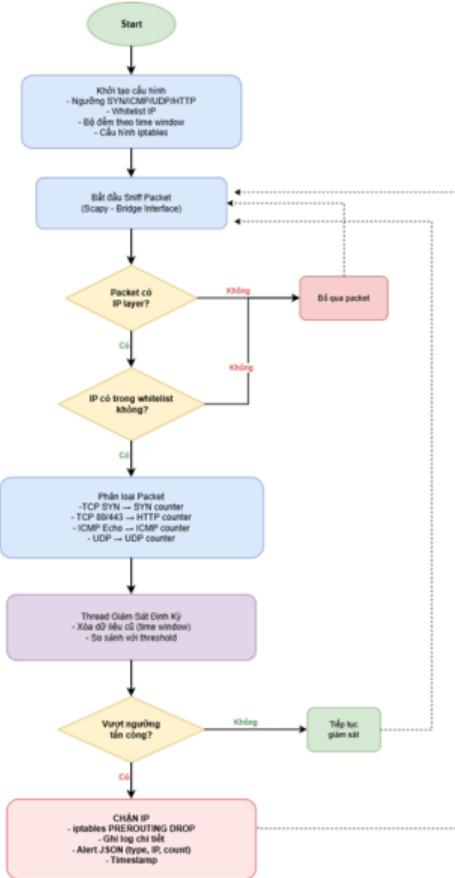
Lưu đồ Tshark Probe

# Kịch bản tấn công



Minh họa kịch bản tấn công

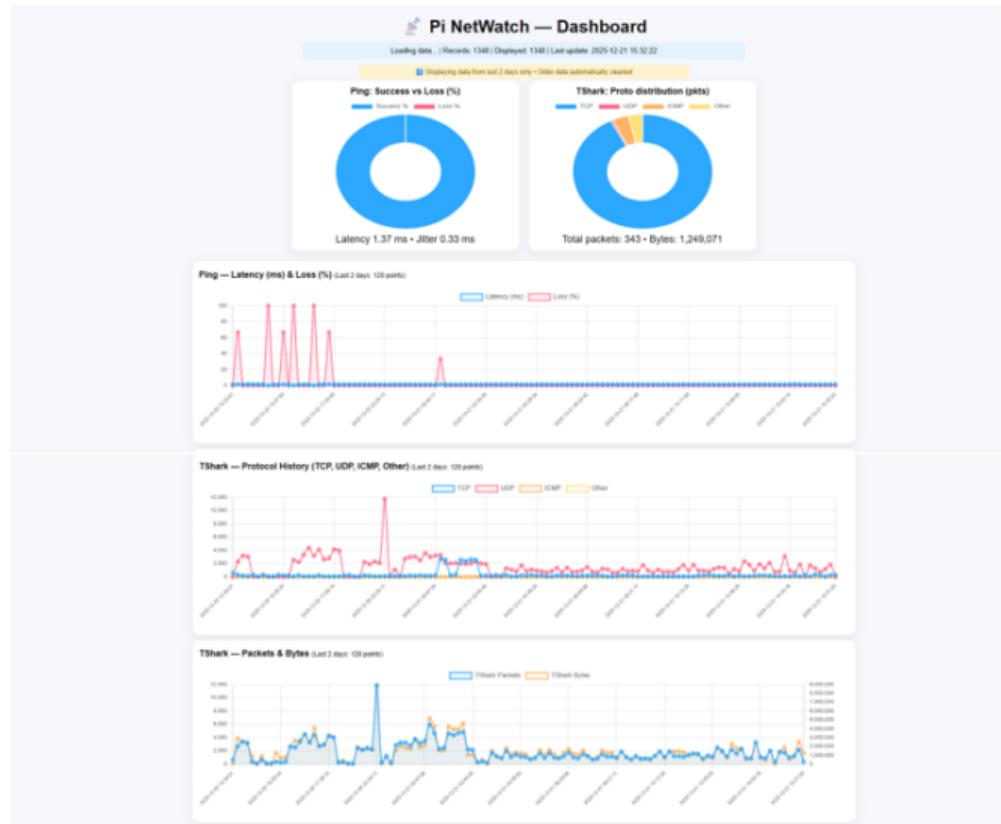
# Lưu đồ thuật toán phương pháp chặn IP



# Mục lục

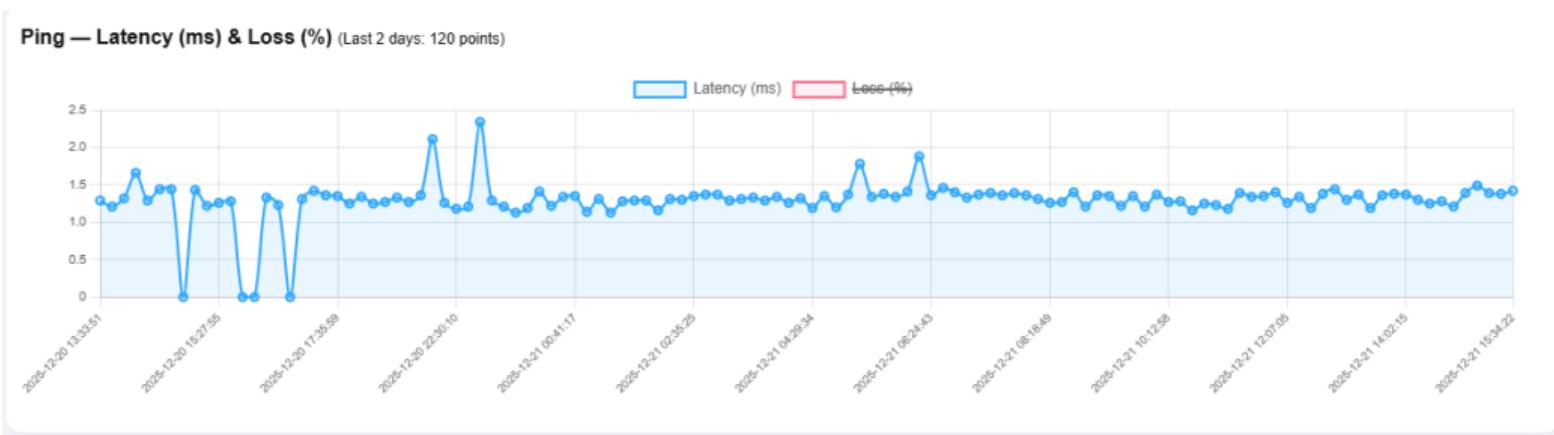
- 1 Giới thiệu
- 2 Mục tiêu đề tài
- 3 Phần cứng và thiết kế
- 4 Phương pháp thực hiện
- 5 Kết quả thực nghiệm
- 6 Kết luận
- 7 Tài liệu tham khảo

# Dashboard Pi NetWatch



Giao diện Dashboard

## Kết quả giám sát - Độ trễ



## Biểu đồ độ trễ

# Kết quả giám sát - Mất gói

Ping — Latency (ms) & Loss (%) (Last 2 days: 120 points)



Tỉ lệ mất gói

# Phân bố giao thức - TCP

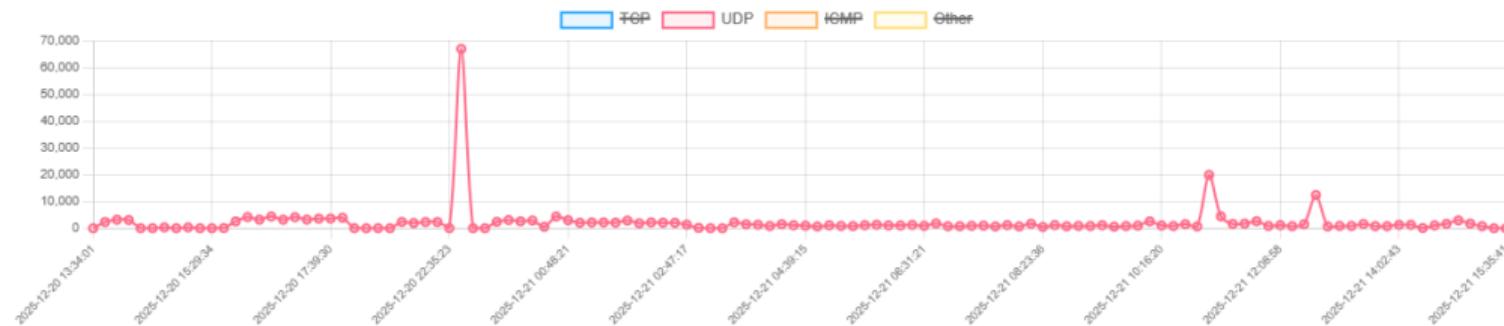
TShark — Protocol History (TCP, UDP, ICMP, Other) (Last 2 days: 120 points)



Lưu lượng TCP

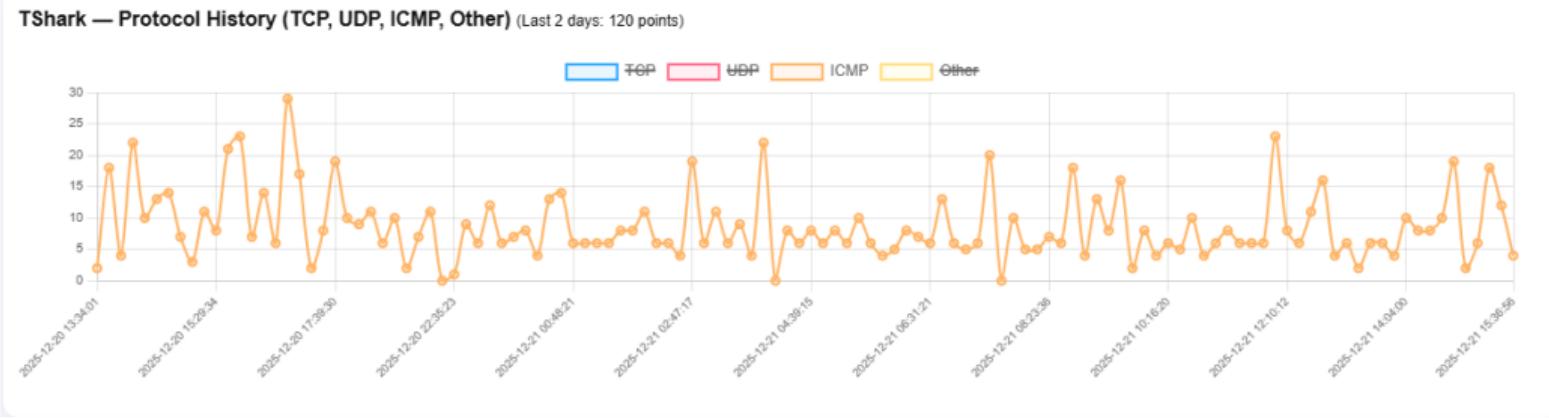
# Phân bố giao thức - UDP

TShark — Protocol History (TCP, UDP, ICMP, Other) (Last 2 days: 120 points)



Lưu lượng UDP

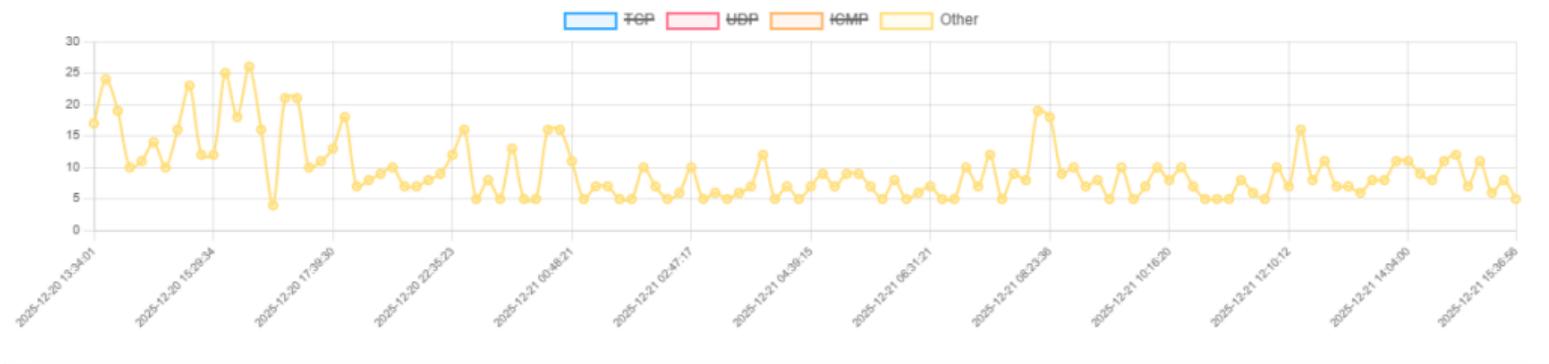
# Phân bố giao thức - ICMP



Lưu lượng ICMP

# Phân bố giao thức - Others

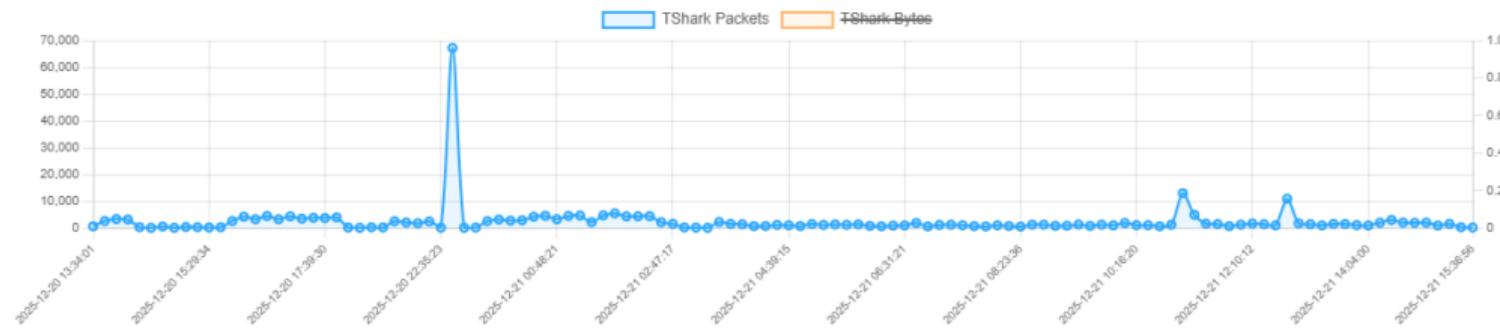
TShark — Protocol History (TCP, UDP, ICMP, Other) (Last 2 days: 120 points)



Các giao thức khác

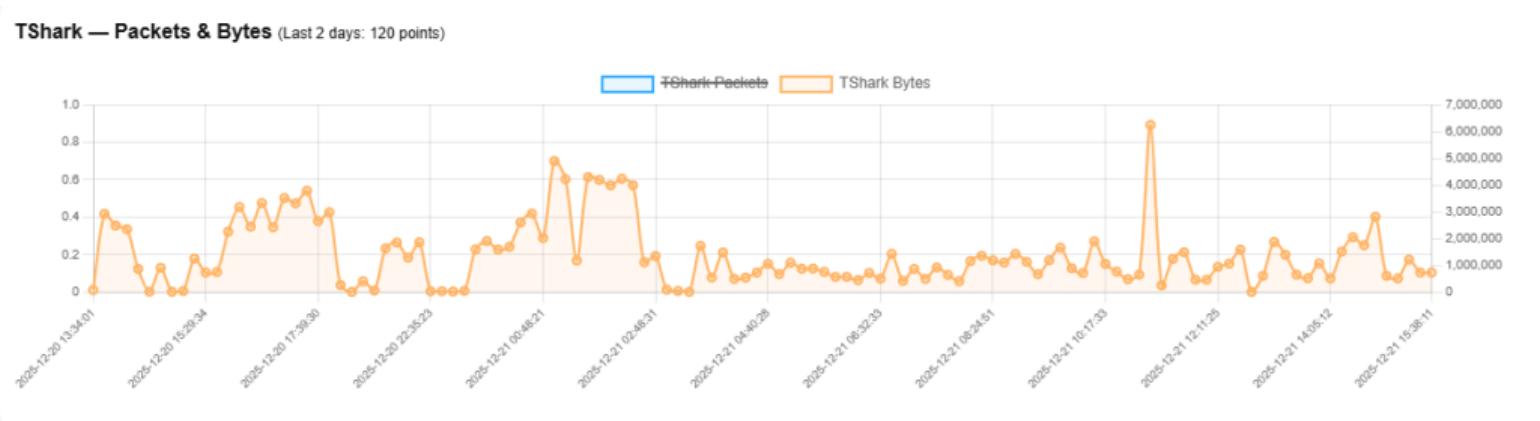
# Lưu lượng tổng - Packets

TShark — Packets & Bytes (Last 2 days: 120 points)



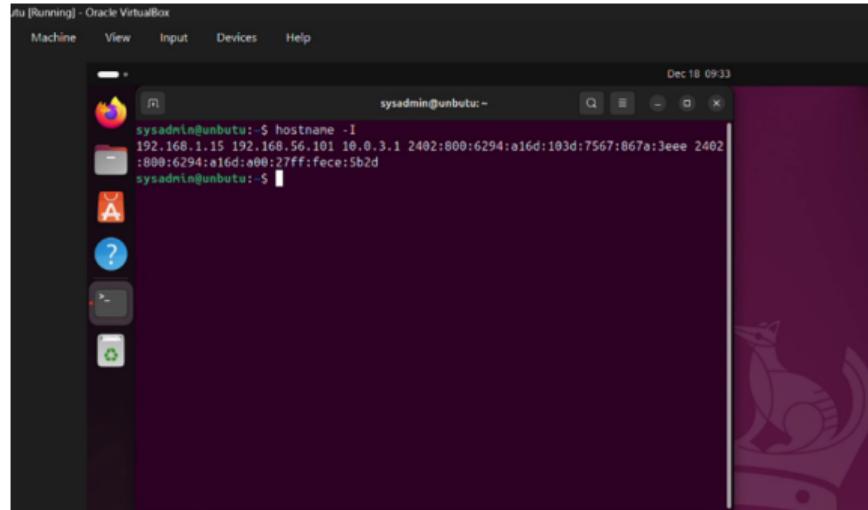
Tổng gói

## Lưu lượng tổng - Bytes



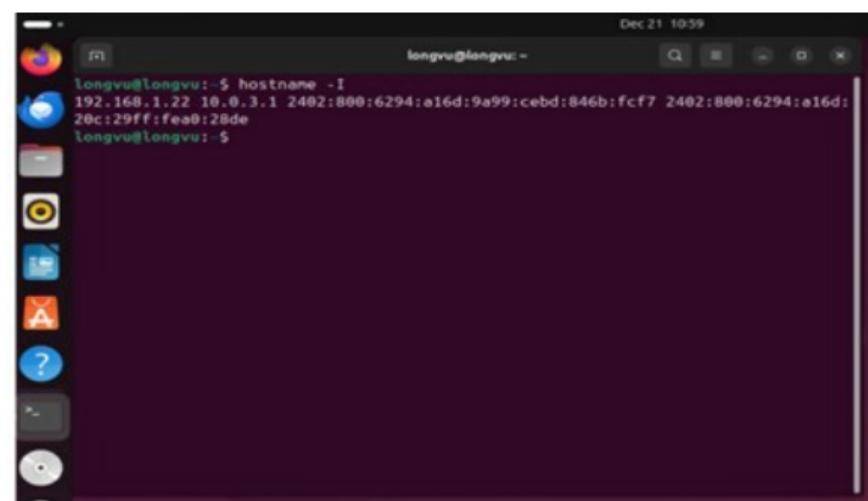
### Tổng Bytes

# Setup chặn IP - Thông tin địa chỉ IP



A screenshot of a Linux desktop environment, likely Ubuntu, running in Oracle VM VirtualBox. The desktop has a dark theme with a purple cat icon in the center. A terminal window titled 'Terminal' is open, showing the command 'hostname -I' and its output: '192.168.1.15 192.168.56.101 10.0.3.1 2402:800:6294:a16d:103d:7567:867a:3eee 2402:800:6294:a16d:a00:27ff:fece:5b2d'. The terminal window has a dark background with light-colored text. The top bar shows the title 'Terminal [Running] - Oracle VirtualBox' and the date 'Dec 18 09:33'.

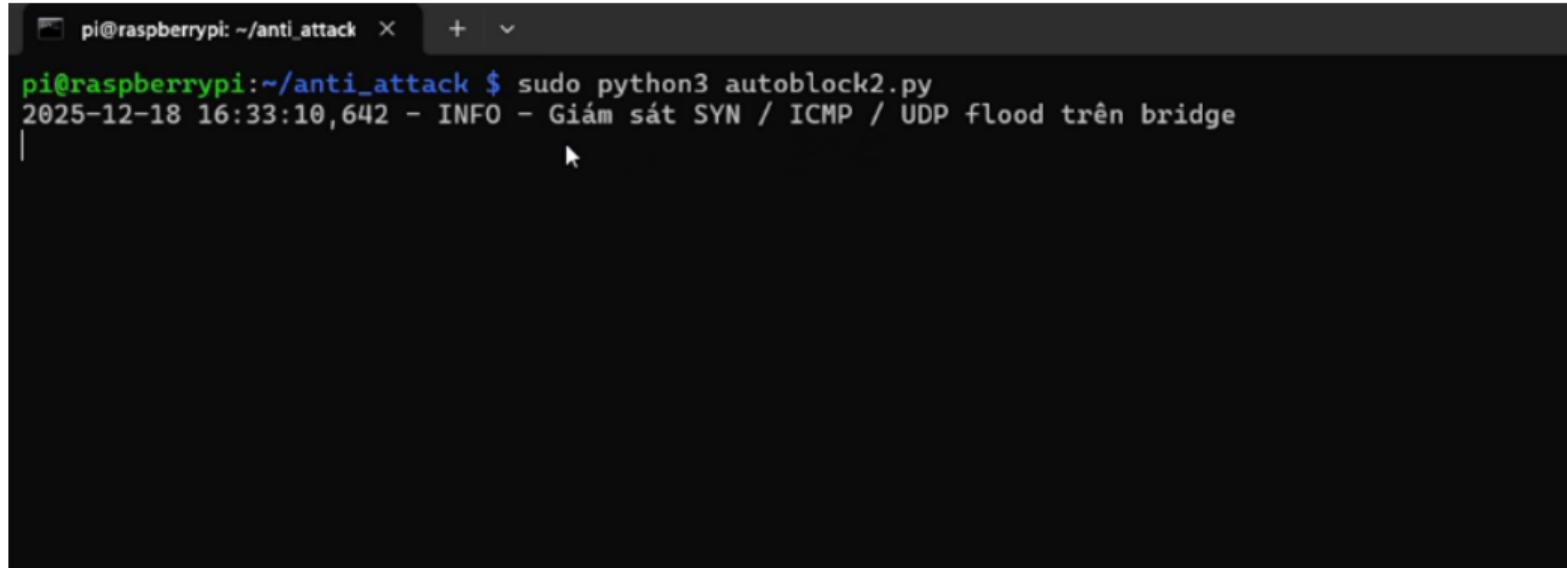
IP máy tấn công  
192.168.1.15



A screenshot of a Linux desktop environment, likely Kali Linux, running in Oracle VM VirtualBox. The desktop has a dark theme with a purple cat icon in the center. A terminal window titled 'Terminal' is open, showing the command 'hostname -I' and its output: '192.168.1.22 10.0.3.1 2402:800:6294:a16d:9a99:cebd:846b:fcd7 2402:800:6294:a16d:20c:29ff:fea0:28de'. The terminal window has a dark background with light-colored text. The top bar shows the title 'Terminal [Running] - Oracle VirtualBox' and the date 'Dec 21 10:59'.

IP máy Server  
192.168.1.22

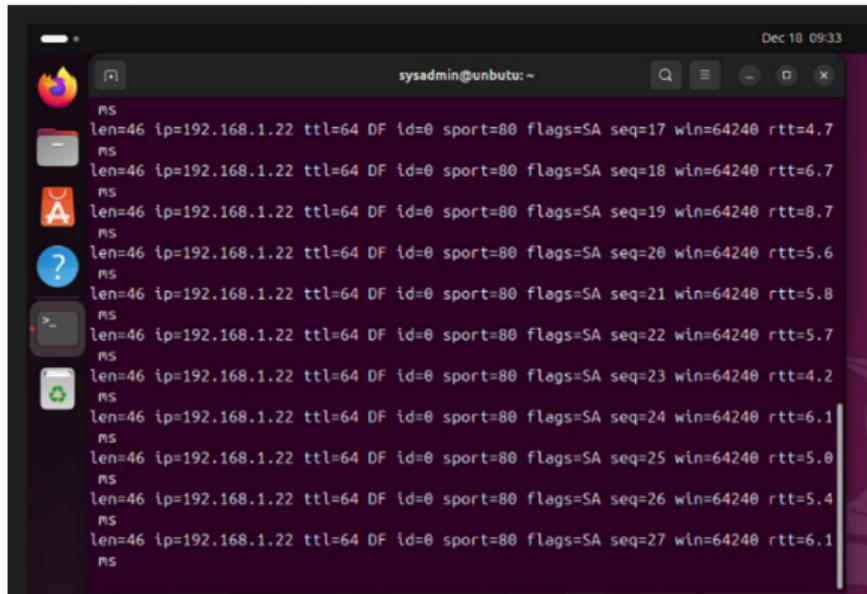
# Pi đang ở chế độ quan sát



```
pi@raspberrypi: ~/anti_attack $ sudo python3 autoblock2.py
2025-12-18 16:33:10,642 - INFO - Giám sát SYN / ICMP / UDP flood trên bridge
```

Chế độ quan sát của pi

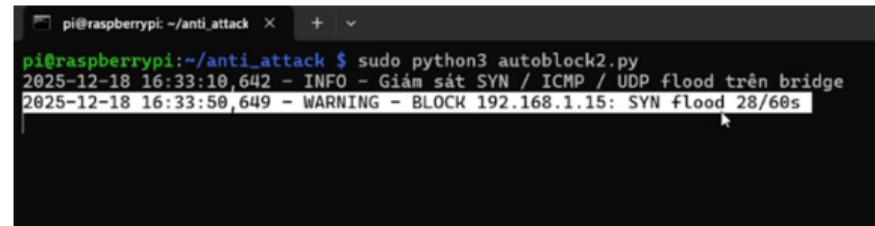
# Kết quả chặn IP - SYN Flood



sysadmin@unbutu:~ Dec 18 09:33

```
MS len=46 ip=192.168.1.22 ttl=64 DF id=0 sport=80 flags=SA seq=17 win=64240 rtt=4.7
MS len=46 ip=192.168.1.22 ttl=64 DF id=0 sport=80 flags=SA seq=18 win=64240 rtt=6.7
MS len=46 ip=192.168.1.22 ttl=64 DF id=0 sport=80 flags=SA seq=19 win=64240 rtt=8.7
MS len=46 ip=192.168.1.22 ttl=64 DF id=0 sport=80 flags=SA seq=20 win=64240 rtt=5.6
MS len=46 ip=192.168.1.22 ttl=64 DF id=0 sport=80 flags=SA seq=21 win=64240 rtt=5.8
MS len=46 ip=192.168.1.22 ttl=64 DF id=0 sport=80 flags=SA seq=22 win=64240 rtt=5.7
MS len=46 ip=192.168.1.22 ttl=64 DF id=0 sport=80 flags=SA seq=23 win=64240 rtt=4.2
MS len=46 ip=192.168.1.22 ttl=64 DF id=0 sport=80 flags=SA seq=24 win=64240 rtt=6.1
MS len=46 ip=192.168.1.22 ttl=64 DF id=0 sport=80 flags=SA seq=25 win=64240 rtt=5.0
MS len=46 ip=192.168.1.22 ttl=64 DF id=0 sport=80 flags=SA seq=26 win=64240 rtt=5.4
MS len=46 ip=192.168.1.22 ttl=64 DF id=0 sport=80 flags=SA seq=27 win=64240 rtt=6.1
```

Log máy tấn công

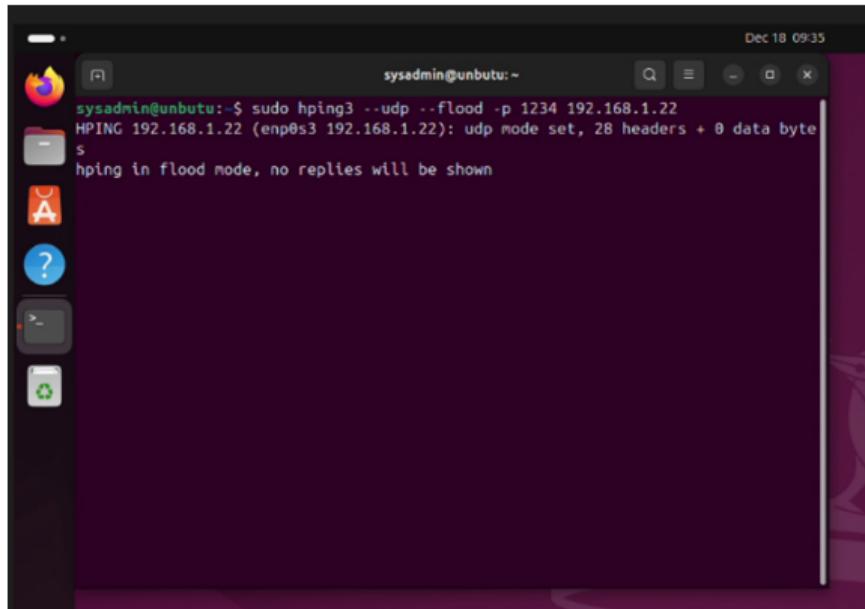


pi@raspberrypi:~/anti\_attack \$ sudo python3 autoblock2.py

```
2025-12-18 16:33:10,642 - INFO - Giám sát SYN / ICMP / UDP flood trên bridge
2025-12-18 16:33:50,649 - WARNING - BLOCK 192.168.1.15: SYN flood 28/60s
```

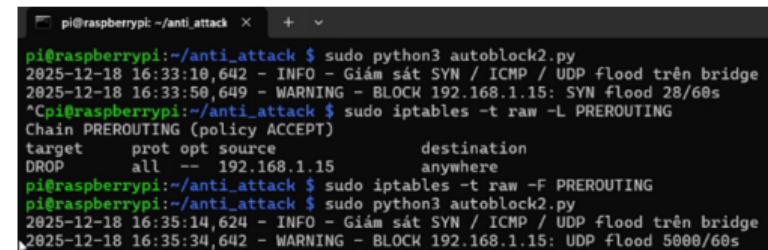
Log Pi - Chặn tại ngưỡng 20

# Kết quả chặn IP - UDP Flood



```
sysadmin@unbutu:~$ sudo hping3 --udp --flood -p 1234 192.168.1.22
HPING 192.168.1.22 (enp0s3 192.168.1.22): udp mode set, 28 headers + 0 data byte
s
hping in flood mode, no replies will be shown
```

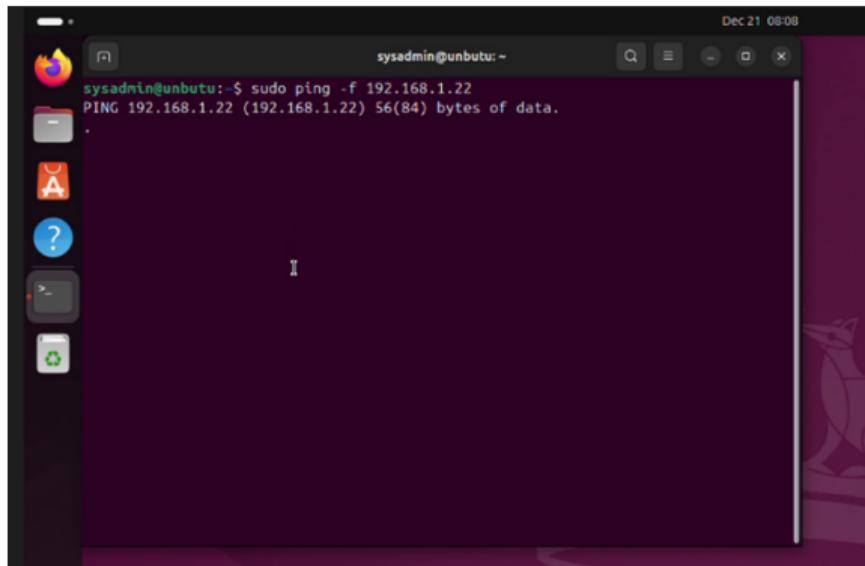
Log máy tấn công



```
pi@raspberrypi:~/anti_attack $ sudo python3 autoblock2.py
2025-12-18 16:33:10,642 - INFO - Giám sát SYN / ICMP / UDP flood trên bridge
2025-12-18 16:33:50,649 - WARNING - BLOCK 192.168.1.15: SYN flood 28/60s
^Cpi@raspberrypi:~/anti_attack $ sudo iptables -t raw -L PREROUTING
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
DROP     all  --  192.168.1.15   anywhere
pi@raspberrypi:~/anti_attack $ sudo iptables -t raw -F PREROUTING
pi@raspberrypi:~/anti_attack $ sudo python3 autoblock2.py
2025-12-18 16:35:14,624 - INFO - Giám sát SYN / ICMP / UDP flood trên bridge
2025-12-18 16:35:34,642 - WARNING - BLOCK 192.168.1.15: UDP flood 5000/60s
```

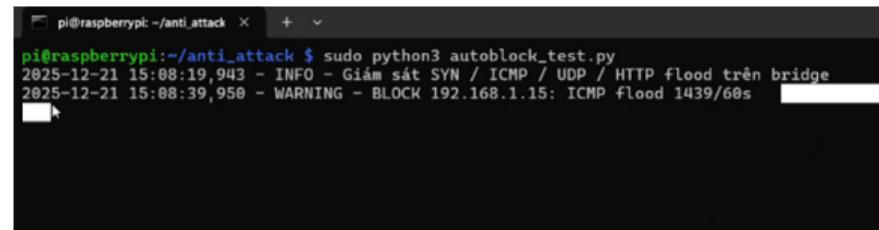
Log Pi - Chặn tại ngưỡng 5000

# Kết quả chặn IP - ICMP Flood



sysadmin@unbutu:~\$ sudo ping -f 192.168.1.22  
PING 192.168.1.22 (192.168.1.22) 56(84) bytes of data.

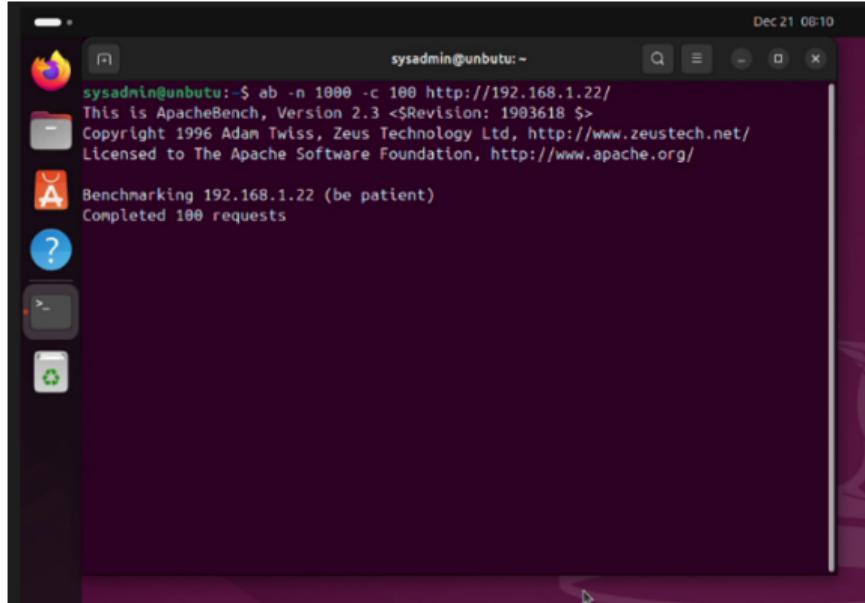
Log máy tấn công



pi@raspberrypi:~/anti\_attack \$ sudo python3 autoblock\_test.py  
2025-12-21 15:08:19,943 - INFO - Giám sát SYN / ICMP / UDP / HTTP flood trên bridge  
2025-12-21 15:08:39,950 - WARNING - BLOCK 192.168.1.15: ICMP flood 1439/60s

Log Pi - Phát hiện và chặn

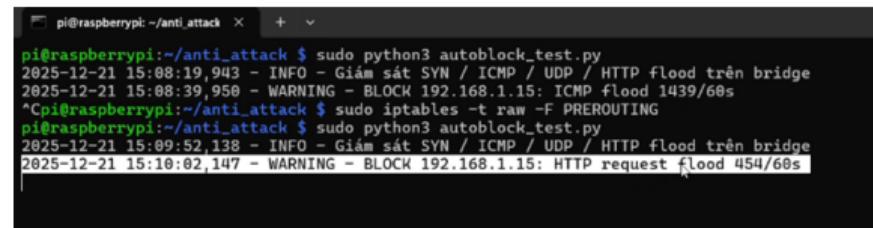
# Kết quả chặn IP - HTTP Flood



```
sysadmin@unbutu:~$ ab -n 1000 -c 100 http://192.168.1.22/
This is ApacheBench, Version 2.3 <$Revision: 1903618 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking 192.168.1.22 (be patient)
Completed 100 requests
```

Log máy tấn công



```
pi@raspberrypi:~/anti_attack $ sudo python3 autoblock_test.py
2025-12-21 15:08:19,943 - INFO - Giám sát SYN / ICMP / UDP / HTTP flood trên bridge
2025-12-21 15:08:39,950 - WARNING - BLOCK 192.168.1.15: ICMP flood 1439/60s
^Cpi@raspberrypi:~/anti_attack $ sudo iptables -t raw -F PREROUTING
pi@raspberrypi:~/anti_attack $ sudo python3 autoblock_test.py
2025-12-21 15:09:52,138 - INFO - Giám sát SYN / ICMP / UDP / HTTP flood trên bridge
2025-12-21 15:10:02,147 - WARNING - BLOCK 192.168.1.15: HTTP request flood 454/60s
```

Log Pi - Chặn tại 454 requests

# Demo time

# Mục lục

- 1 Giới thiệu
- 2 Mục tiêu đề tài
- 3 Phần cứng và thiết kế
- 4 Phương pháp thực hiện
- 5 Kết quả thực nghiệm
- 6 **Kết luận**
- 7 Tài liệu tham khảo

## Thực hiện được:

- Xây dựng thành công hệ thống giám sát và quản trị mạng
- Thu thập, phân tích và hiển thị trực quan các thông số mạng
- Hoạt động dưới dạng cầu mạng hiệu quả
- Tích hợp chức năng chặn IP tấn công
- Chi phí thấp, dễ triển khai

## Hạn chế:

- Phụ thuộc vào phần cứng Raspberry Pi
- Thuật toán phát hiện còn đơn giản
- Dashboard chưa hỗ trợ nhiều tương tác nâng cao
- Mới thử nghiệm một số dạng tấn công

# Hướng phát triển

## Các hướng mở rộng trong tương lai:

- Tối ưu hóa hiệu năng hệ thống
- Bổ sung thuật toán phát hiện nâng cao (Machine Learning)
- Hỗ trợ nhiều dạng tấn công khác nhau
- Phát triển dashboard thời gian thực hoàn chỉnh
- Lưu trữ và phân tích dữ liệu lịch sử

# Mục lục

- 1 Giới thiệu
- 2 Mục tiêu đề tài
- 3 Phần cứng và thiết kế
- 4 Phương pháp thực hiện
- 5 Kết quả thực nghiệm
- 6 Kết luận
- 7 Tài liệu tham khảo

## Tài liệu tham khảo

- ① J. Svoboda, I. Ghafir, and V. Prenosil, "Network monitoring approaches: An overview," *Int. J. Adv. Comput. Netw. Secur.*, vol. 5, pp. 88–93, 2015.
- ② K. A. Saeed, D. Wu, and D. J. Xu, "Effect of designer- versus user-driven network-monitoring dashboard design on user flow experience and performance," *Information and Management*, vol. 61, no. 3, 2024.
- ③ R. Shikhaliyev and L. Sukhostat, "Proactive computer network monitoring based on homogeneous deep neural ensemble," *Results in Control and Optimization*, vol. 11, 2023.
- ④ L. L. Ramalho et al., "A SBC-based data acquisition system: A case study on smart reclosers and multiagent systems," *IEEE Access*, vol. 11, pp. 48988–49001, 2023.
- ⑤ C.-D. Chiang et al., "Development of microcontroller-based status monitoring system for diagnosis and prognosis of smart factory," in *Proc. SICE Festival with Annual Conference (SICE FES)*, 2024.
- ⑥ M. Varol and M. İskefiyeli, "A low cost compact network TAP device with Raspberry Pi 4," *Engineering Science and Technology, an International Journal*, vol. 70, no. 102118, 2025.

**Cảm ơn các thầy cô  
và các bạn đã lắng nghe!**



# File pcap dưới dạng hexa

```
pi@raspberrypi:~/pi_netwatch/captures $ hexdump -C pcap_file.pcap | head -n 20
00000000  0a 0d 0d 0a 5c 00 00 00  4d 3c 2b 1a 01 00 00 00  |....\...M<+....|
00000010  ff ff ff ff ff ff ff  03 00 18 00 4c 69 6e 75  |.....Linu|
00000020  78 20 36 2e 31 32 2e 34  37 2b 72 70 74 2d 72 70  |x 6.12.47+rpt-rp|
00000030  69 2d 76 38 04 00 19 00  44 75 6d 70 63 61 70 20  |i-v8....Dumpcap|
00000040  28 57 69 72 65 73 68 61  72 6b 29 20 34 2e 34 2e  |(Wireshark) 4.4.|
00000050  37 00 00 00 00 00 00 00  5c 00 00 00 01 00 00 00  |7.....\.....|
00000060  48 00 00 00 01 00 00 00  00 00 04 00 02 00 07 00  |H.....|
00000070  62 72 69 64 67 65 30 00  09 00 01 00 09 00 00 00  |bridge0.....|
00000080  0c 00 18 00 4c 69 6e 75  78 20 36 2e 31 32 2e 34  |....Linux 6.12.4|
00000090  37 2b 72 70 74 2d 72 70  69 2d 76 38 00 00 00 00  |7+rpt-rpi-v8...|
000000a0  48 00 00 00 06 00 00 00  7c 00 00 00 00 00 00 00  |H.....|.....|
000000b0  ec 7b 83 18 85 4f 8a 76  5a 00 00 00 5a 00 00 00  |.{...0.vZ...Z..|
000000c0  5e 0d e0 97 13 7e f8 b5  4d fa 5b ef 08 00 45 00  |^....~..M.[...E.|
000000d0  00 4c 6d 95 40 00 80 06  09 b8 c0 a8 01 04 c0 a8  |.Lm.@.....|
000000e0  01 0a cf 2b 00 16 67 7f  27 cc 4b bb 71 f5 50 18  |...+..g.'..K.q.P.|
000000f0  00 ff 12 ca 00 00 6b f5  b8 bb 07 4d 5d 5b 8d fe  |.....k....M][..|
00000100  9c 36 8e 8f 74 43 36 4c  5c b3 dc 36 e6 17 2f 15  |.6..tC6L\..6../.|
00000110  da 3a cc 34 b8 7d 47 2c  1b 64 00 00 7c 00 00 00  |.:4.}G,.d..|..|
00000120  06 00 00 00 7c 00 00 00  00 00 00 00 ec 7b 83 18  |....|.....{..|
00000130  24 5f 8d 76 5a 00 00 00  5a 00 00 00 f8 b5 4d fa  |$_.vZ...Z....M.|
```

# File pcap dưới dạng tshark

```
pi@raspberrypi:~/pi_netwatch/captures $ tshark -r pcap_file.pcap
1 0.000000000 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
2 0.000200607 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
3 0.030708385 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
4 0.030793439 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
5 0.060809411 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
6 0.060952612 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
7 0.072473351 34.120.52.64 → 192.168.1.12 TLSv1.2 115 Application Data
8 0.092689588 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
9 0.092761142 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
10 0.123110886 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
11 0.123175718 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
12 0.126609892 192.168.1.12 → 34.120.52.64 TCP 60 58119 → 443 [ACK] Seq=1 Ack=62 Win=253 Len=0
13 0.153651385 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
14 0.153715440 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
15 0.184339178 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
16 0.184468527 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
17 0.215582238 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
18 0.215658144 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
19 0.260629585 192.168.1.4 → 192.168.1.10 TCP 60 53035 → 22 [ACK] Seq=289 Ack=289 Win=253 Len=0
20 0.260630307 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
21 0.260798785 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
22 0.306972962 192.168.1.4 → 192.168.1.10 TCP 60 53035 → 22 [ACK] Seq=325 Ack=325 Win=253 Len=0
23 0.321604289 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
24 0.321670492 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
25 0.367493602 192.168.1.4 → 192.168.1.10 TCP 60 53035 → 22 [ACK] Seq=361 Ack=361 Win=253 Len=0
26 0.367494102 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
27 0.367640562 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
28 0.378893121 26:01:2a:32:4e:b0 → Spanning-tree-(for-bridges)_00 STP 60 Conf. Root = 0/0:24:0b:2a:32:4e:b0 Cost = 0 Port = 0x8002
29 0.399006106 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
30 0.399072395 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
31 0.429685579 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
32 0.429754762 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
33 0.460770049 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
34 0.461511831 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
35 0.491358399 192.168.1.4 → 192.168.1.10 SSH 90 Client: Encrypted packet (len=36)
36 0.491433453 192.168.1.10 → 192.168.1.4 SSH 90 Server: Encrypted packet (len=36)
37 0.500845159 192.168.1.10 → 192.168.1.4 SSH 98 Server: Encrypted packet (len=44)
38 0.5030894523 192.168.1.4 → 192.168.1.10 TCP 60 53035 → 22 [ACK] Seq=541 Ack=585 Win=252 Len=0
```



## File json

```
[{"_index": "packets-2025-12-22",
 "_type": "doc",
 "_score": null,
 "_source": {
   "layers": {
     "frame": {
       "frame.section_number": "1",
       "frame.interface_id": "0",
       "frame.interface_id_tree": {
         "frame.interface_name": "bridge0"
       },
       "frame.encap_type": "1",
       "frame.time": "Dec 22, 2025 15:22:14.390640517 +07",
       "frame.time_utc": "Dec 22, 2025 08:22:14.390640517 UTC",
       "frame.time_epoch": "1766391734.390640517",
       "frame.offset_shift": "0.000000000",
       "frame.time_delta": "0.000000000",
       "frame.time_delta_displayed": "0.000000000",
       "frame.time_relative": "0.000000000",
       "frame.number": "1",
       "frame.len": "90",
       "frame.cap_len": "90",
       "frame.marked": "0",
       "frame.ignored": "0",
       "frame.protocols": "eth:ethertype:ip:tcp:ssh"
     },
     "eth": {
       "eth.dst": "5e:0d:e0:97:13:7e",
       "eth.dst_tree": {
         "eth.dst_resolved": "5e:0d:e0:97:13:7e",
         "eth.dst.oui": "6163936",
         "eth.dst.lg": "1",
         "eth.dst.ig": "0",
         "eth.addr": "5e:0d:e0:97:13:7e",
         "eth.addr_resolved": "5e:0d:e0:97:13:7e"
       }
     }
   }
 }
```