Họ tên: Trần Trí Dũng

MSSV: HE190680

Lớp: IA1901

11.1 – Installing Logwatch

**Cấu hình chuyển tiếp**:

* Đã cấu hình việc chuyển tiếp thư từ người dùng root đến tài khoản người dùng thông thường (dungtt-he190630) thông qua tệp /etc/aliases
* Lệnh newaliases đã áp dụng cấu hình này thành công

**Hệ thống cron**:

* Thư hiển thị là từ "Cron Daemon", cho biết hệ thống cron đang chạy tác vụ định kỳ
* Cụ thể là đang chạy các script trong thư mục /etc/cron.hourly (các tác vụ được lên lịch chạy hàng giờ)

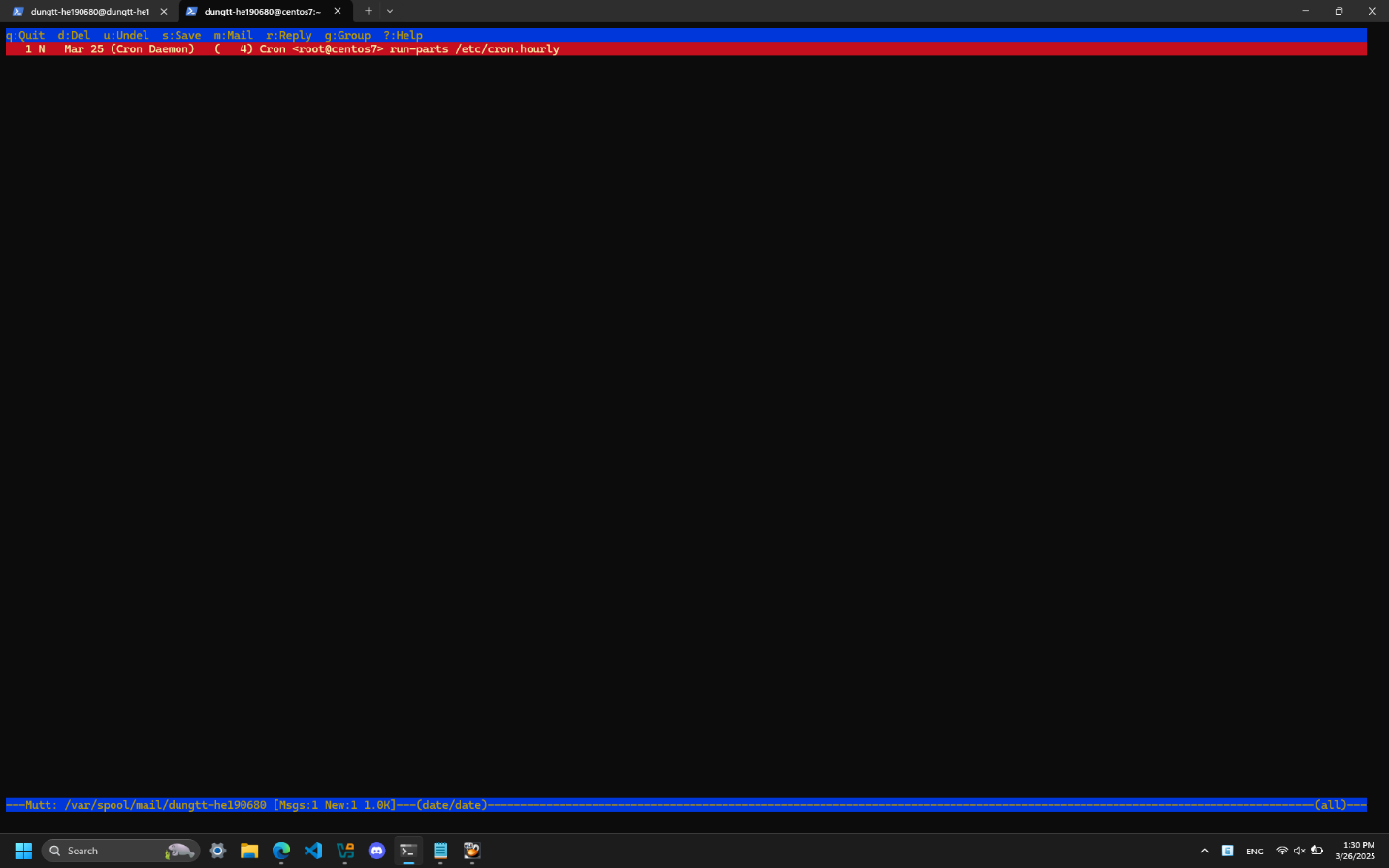
**Postfix**:

* Hệ thống mail nội bộ Postfix đã được cấu hình đúng và đang hoạt động
* Nó đã gửi thông báo từ cron đến người dùng

**Mutt**:

* Trình đọc thư mutt đã được cài đặt và cấu hình đúng
* Có thể xem các thư hệ thống thông qua giao diện này

Do chưa đến thời điểm Logwatch gửi báo cáo hàng ngày nên không hiển thị báo cáo từ Logwatch, nhưng kết quả cho thấy hệ thống mail nội bộ đã hoạt động đúng.



11.2 – Setting up a basic log server

**Tập trung log**:

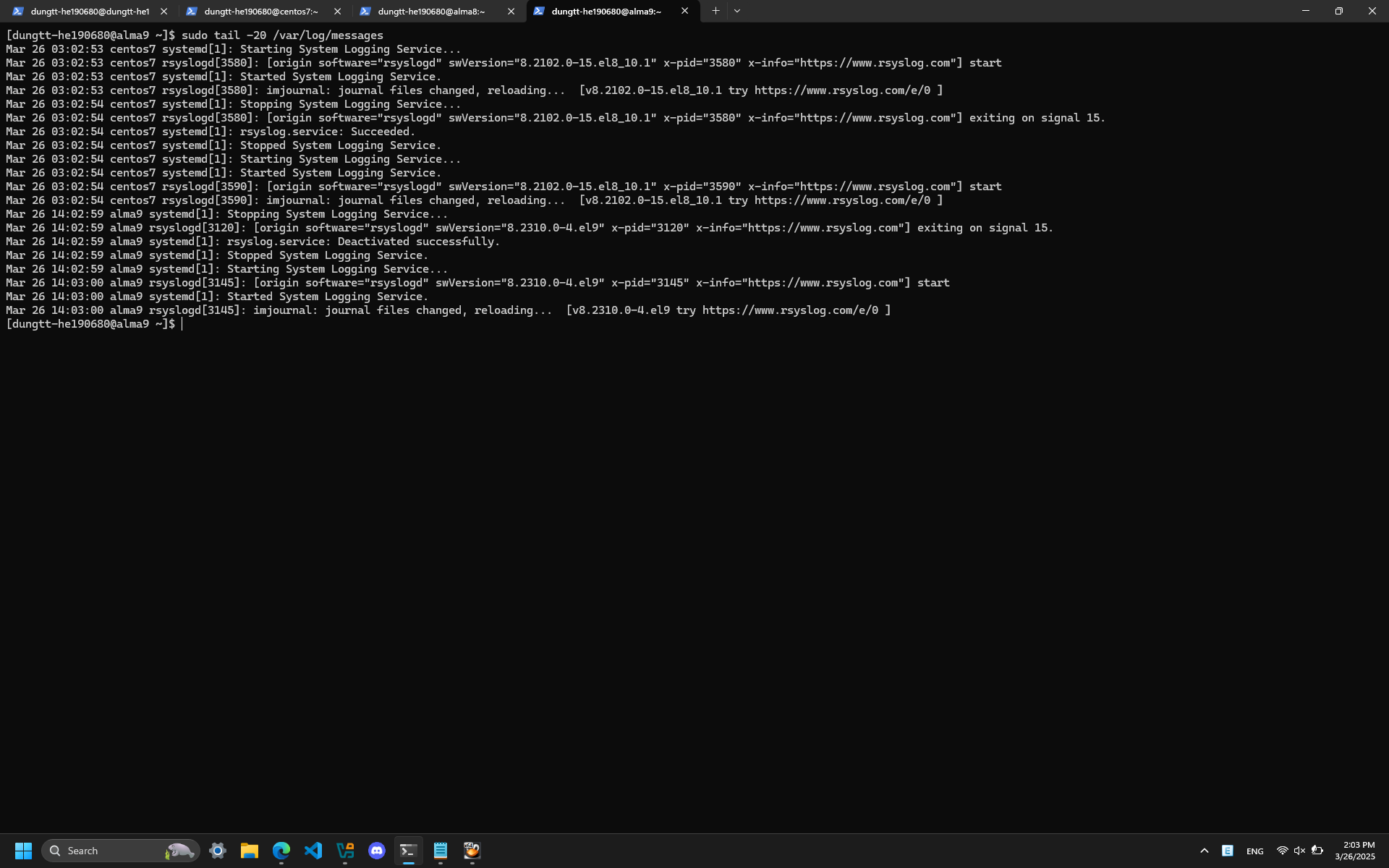
* Log từ cả hai máy chủ (centos7 và alma9) đều xuất hiện trong cùng một tệp /var/log/messages trên máy chủ đang xem log.
* Chứng tỏ cấu hình rsyslog đã hoạt động đúng, cho phép một máy chủ thu thập log từ nhiều máy khác nhau.

**Hoạt động của rsyslog**:

* Các dòng nhật ký cho thấy dịch vụ rsyslog đã khởi động, dừng và khởi động lại trên cả hai máy chủ.
* Có thể thấy các thông báo như "Starting System Logging Service", "Stopped System Logging Service" và "Started System Logging Service".

**Phiên bản rsyslog khác nhau**:

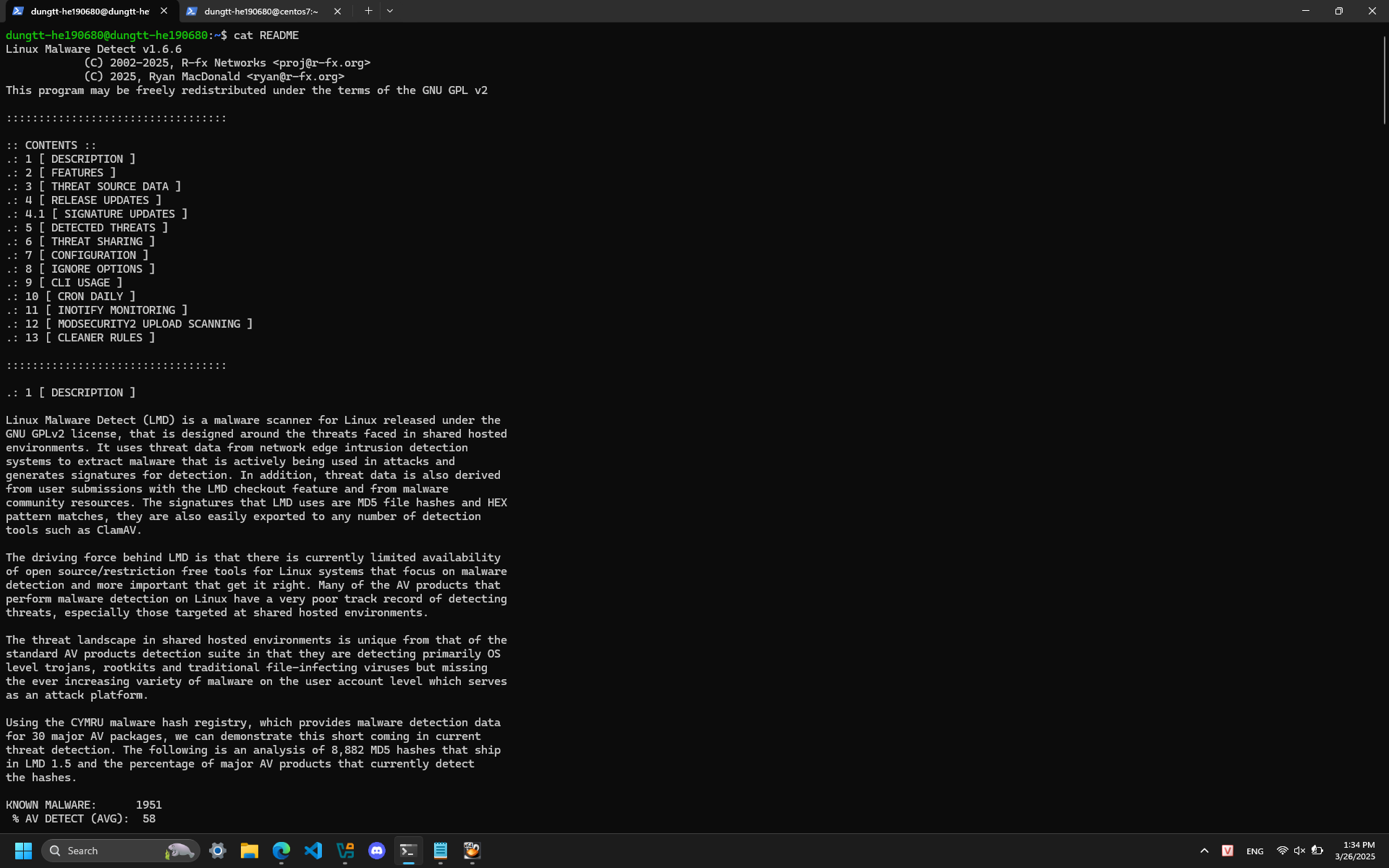
* Trên centos7: sử dụng rsyslog phiên bản 8.2102.0-15.el8\_10.1
* Trên alma9: sử dụng rsyslog phiên bản 8.2310.0-4.el9
* Điều này cho thấy hai hệ thống đang chạy các phiên bản khác nhau của rsyslog nhưng vẫn có thể giao tiếp và chia sẻ nhật ký với nhau.



12.1 – Installing ClamAV and maldet

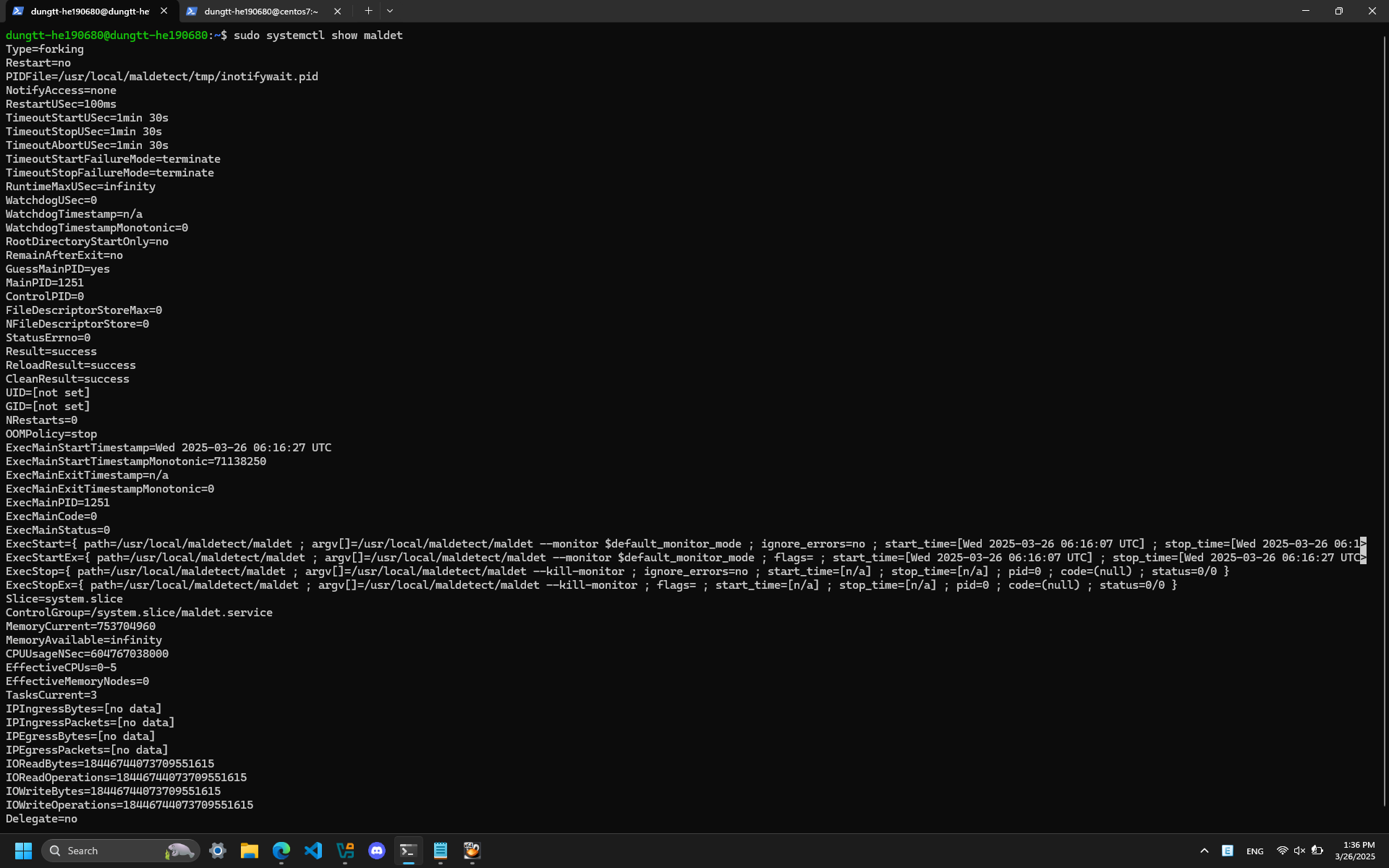
**Nội dung chính của file README:** Thông tin cơ bản, Mô tả, Động lực phát triển, Hiệu quả phát hiện, Cấu trúc tài liệu, …

File README này là tài liệu tham khảo quan trọng khi sử dụng LMD để bảo vệ hệ thống Linux khỏi các mối đe dọa malware, đặc biệt trong môi trường hosting chia sẻ.



12.2 – Configuring maldet

Kết quả này cho thấy dịch vụ maldet đã được khởi động thành công sau khi thực hiện các bước cấu hình. Dịch vụ đang chạy và giám sát các thư mục đã cấu hình trong file /usr/local/maldetect/monitor\_paths (bao gồm /var/tmp, /tmp, /home, và /root như đã thiết lập).



12.4 – Using auditd

**Quy tắc theo dõi file passwd**:

* -w /etc/passwd: Theo dõi file /etc/passwd
* -p wa: Giám sát các hoạt động ghi (w) và thay đổi thuộc tính (a)
* -k passwd\_changes: Gắn từ khóa "passwd\_changes" để dễ dàng tìm kiếm trong log

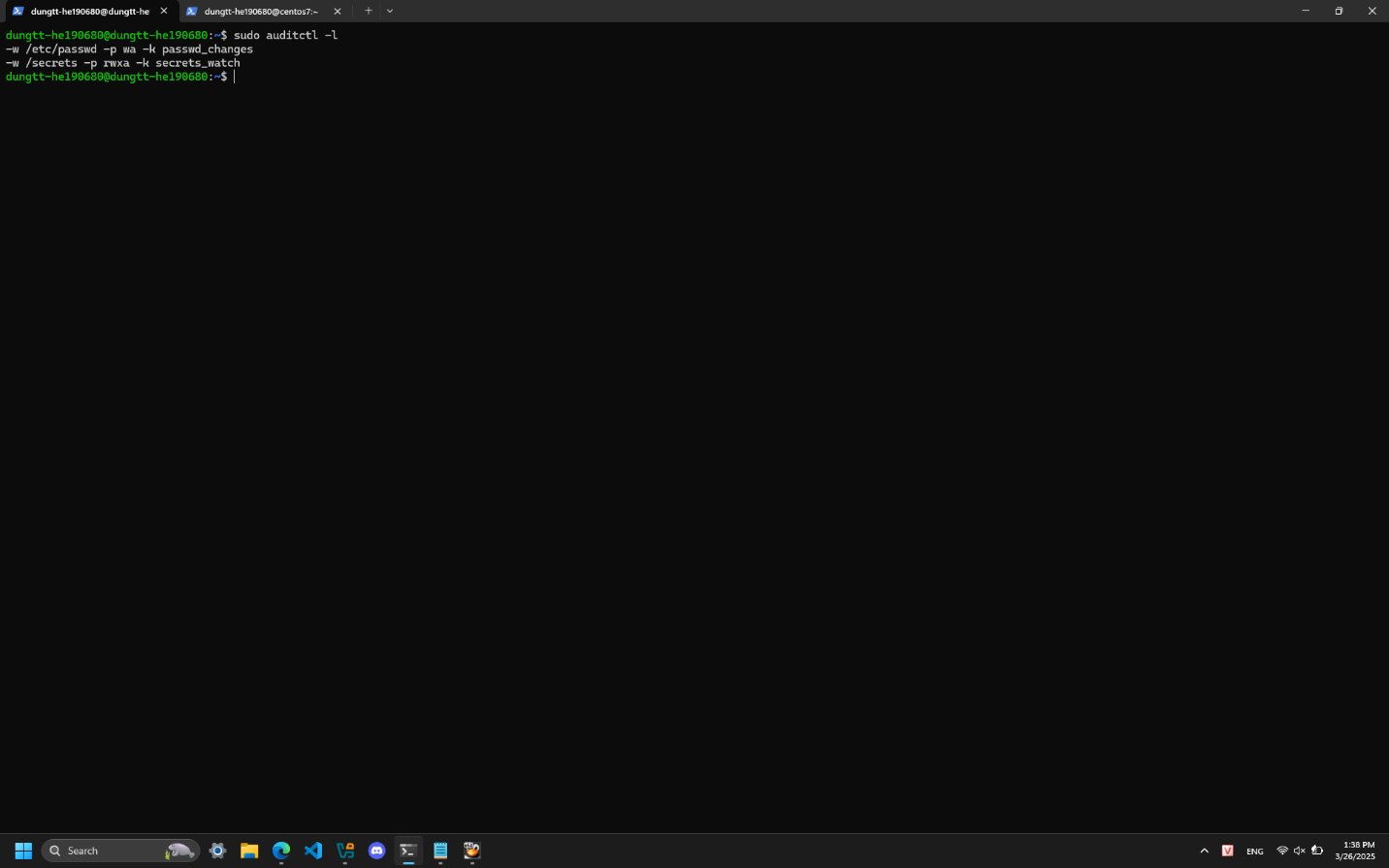
**Quy tắc theo dõi thư mục secrets**:

* -w /secrets: Theo dõi thư mục /secrets
* -p rwxa: Giám sát đầy đủ các hoạt động
* -k secrets\_watch: Gắn từ khóa "secrets\_watch" cho các sự kiện liên quan

**Tính liên tục của các quy tắc**: Các quy tắc audit đã được lưu thành công thành quy tắc cố định và vẫn còn hiệu lực sau khi khởi động lại hệ thống.

**Mức độ giám sát khác nhau**: Có sự khác biệt trong mức độ giám sát giữa hai quy tắc:

* File /etc/passwd chỉ được giám sát cho hoạt động ghi và thay đổi thuộc tính (wa), vì đây là file hệ thống quan trọng, chỉ quan tâm khi có thay đổi.
* Thư mục /secrets được giám sát toàn diện (rwxa) vì đây là thư mục nhạy cảm và chúng ta muốn biết mọi loại truy cập vào nó.

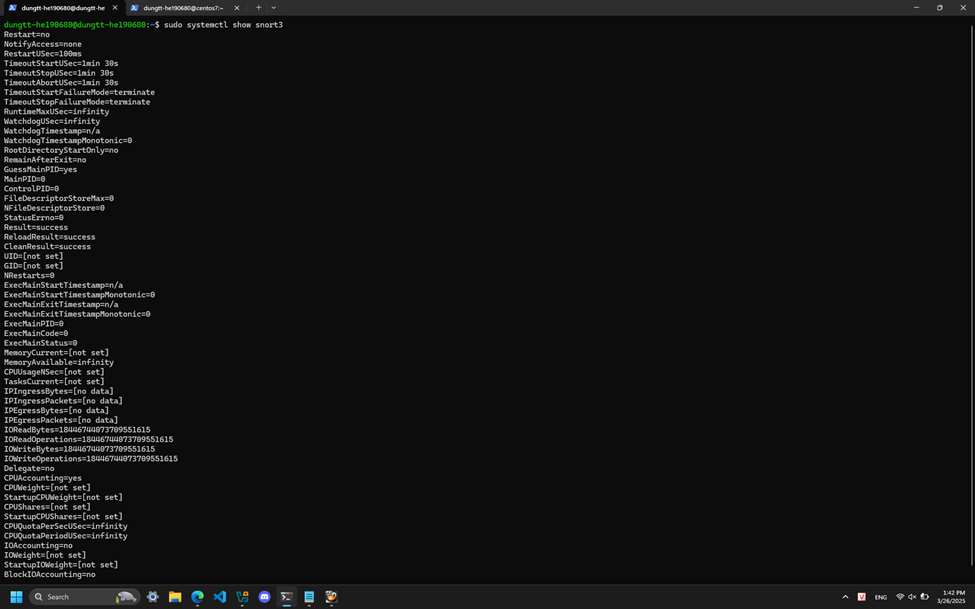


13.1 – Installing Snort via a Docker container

**Trạng thái Dịch vụ**: Kết quả cho thấy dịch vụ Snort3 đã được cài đặt trên hệ thống.

**Cấu hình Dịch vụ**: Snort3 được cấu hình như một dịch vụ systemd, cho phép quản lý thông qua các lệnh systemctl như start, stop, và status.

**Kiểm tra Cài đặt**: Lệnh này được sử dụng để xác nhận rằng Snort3 đã được cài đặt đúng cách trên hệ thống trước khi tiếp tục với các bước tiếp theo trong lab.

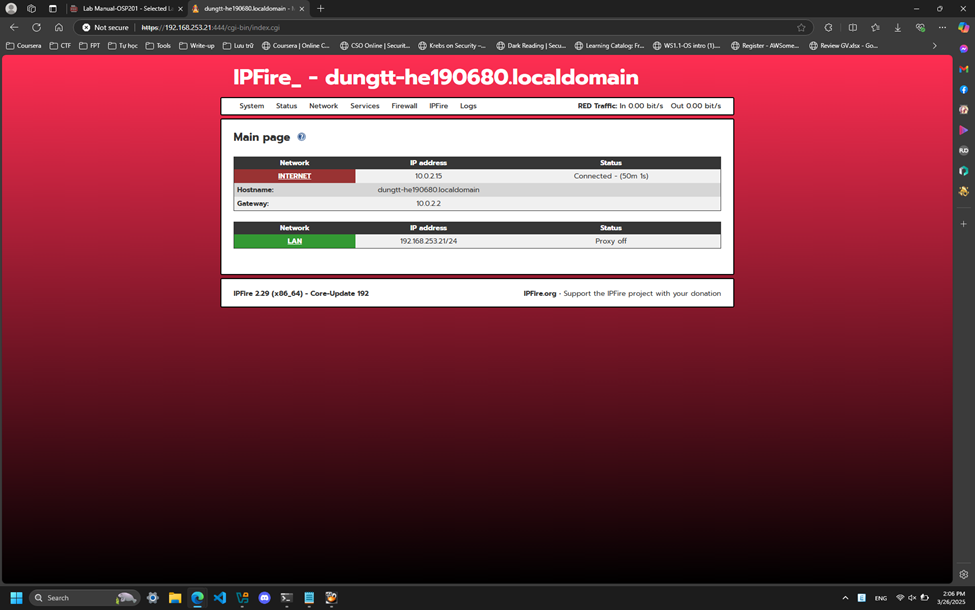


13.2 – Creating an IPFire virtual machine

**Cài đặt IPFire:** Đã cài đặt thành công IPFire trong máy ảo với cấu hình hai giao diện mạng.

**Cấu hình giao diện mạng:** Đã cấu hình giao diện Bridged làm GREEN (mạng nội bộ) và giao diện NAT làm RED (kết nối internet).

**Truy cập giao diện web:** Đã truy cập thành công vào giao diện web quản trị của IPFire qua URL https://192.168.253.21:444 (địa chỉ IP của giao diện GREEN).



13.3 – Installing Nikto from Github

Nikto là một công cụ quét bảo mật web quan trọng trong bộ công cụ kiểm tra bảo mật. Màn hình trợ giúp này cung cấp tổng quan về các khả năng và tùy chọn cấu hình của Nikto.

