Lab Scanning with OpenVas

Chuẩn bị

- Máy Kali có sẵn tool GVM-OpenVAS
- Máy metasploitable2

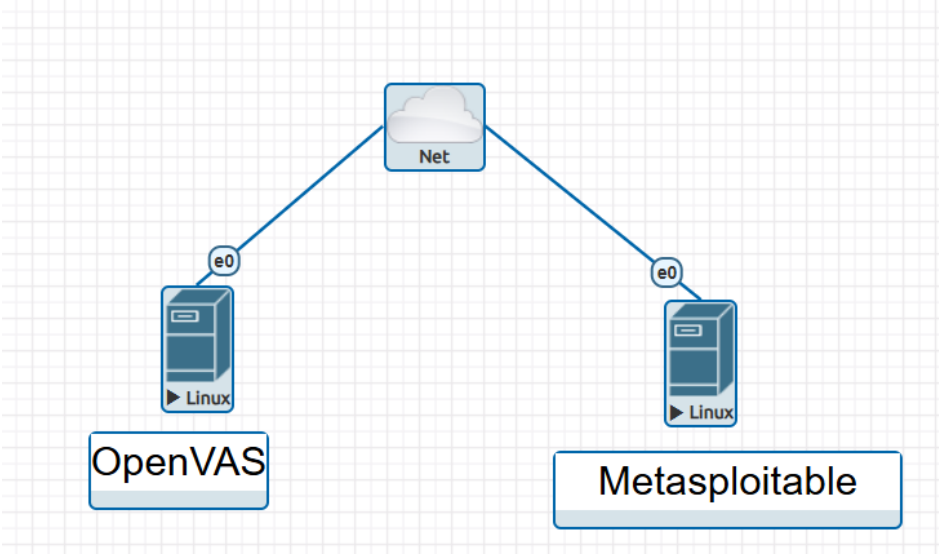
Mục tiêu

- Hiểu và vận hành được công cụ OpenVas.
- Quét, đọc và hiểu các lỗ hổng được phát hiện
- Phân tích kết quả quét, diễn giải các lỗ hổng bảo mật thực tế.

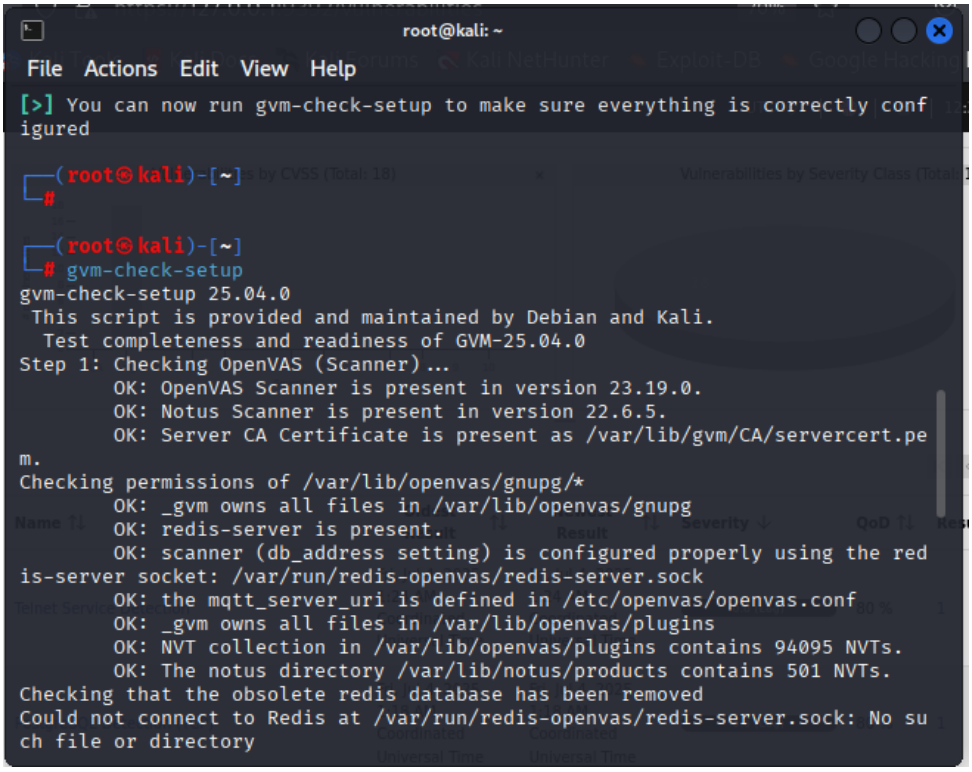
Cảnh báo: Tất cả các bài lab tấn công chỉ được thực hiện trong **môi trường ảo**, **cách ly** và **hợp pháp**. **Tuyệt đối không** áp dụng trên **hệ thống thật** hoặc **mạng không được phép**, mọi vi phạm sẽ bị xử lý theo quy định và pháp luật hiện hành.

Bài tập thực hành

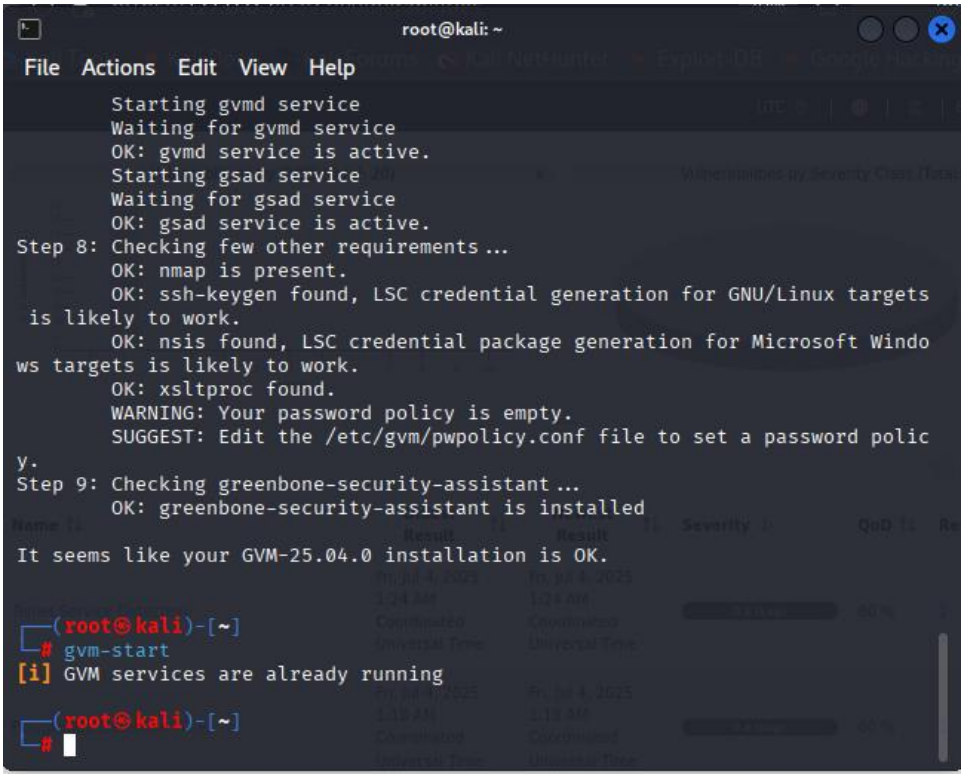
Mô tả: mô hình gồm 2 đối tượng, OpenVAS là máy sử dụng để quét các lỗ hổng và Metasploitable là mục tiêu cần quét cho bài lab này.



Ở trong kali linux dùng câu lệnh gvm-check-setup. Nếu bị báo lỗi, chạy lệnh gvm-setup, rồi chạy lệnh gvm-start.

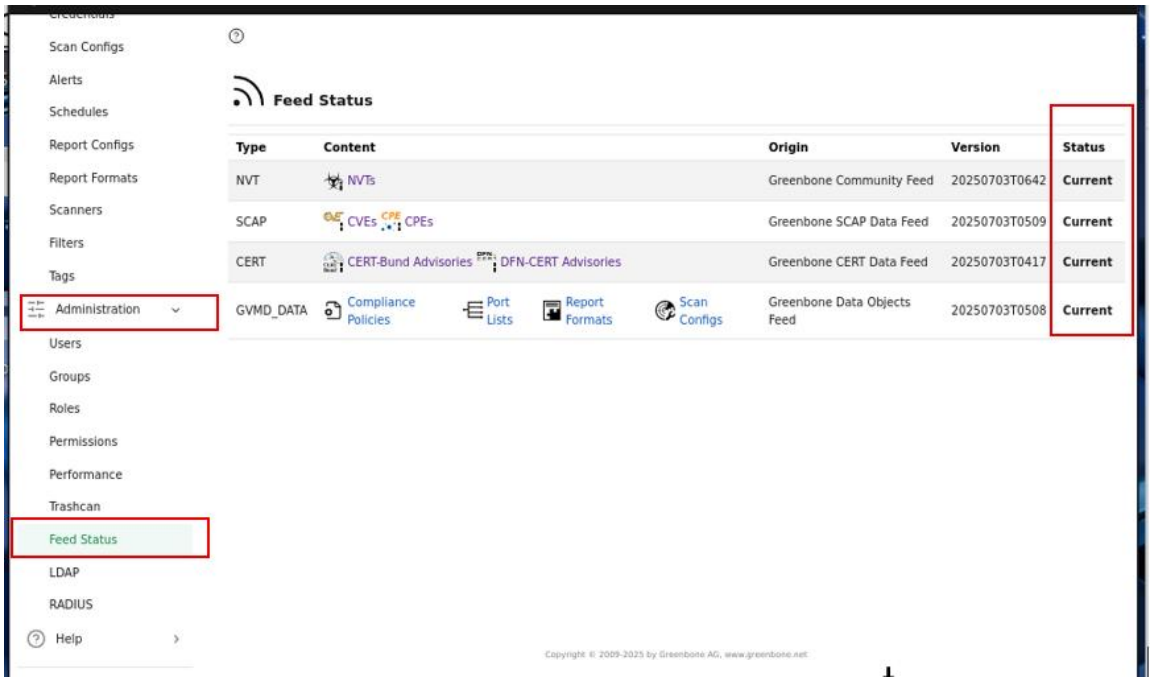


Chạy lệnh gvm-start

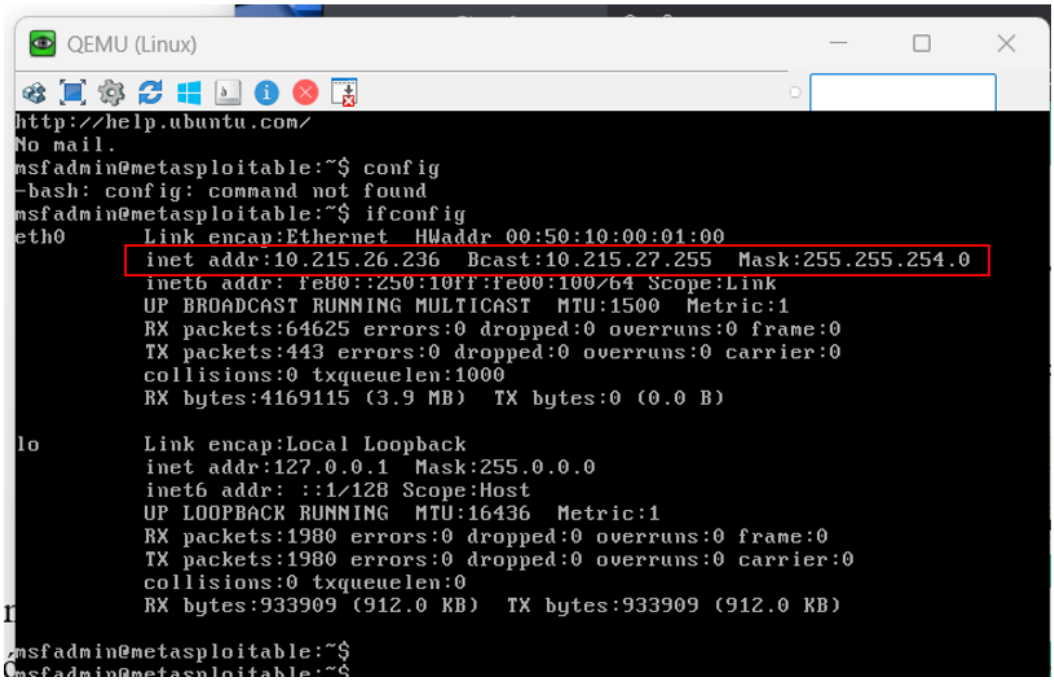


Sau đó sẽ có một trang web xuất hiện, sử dụng tài khoản admin để đăng nhập. ây là giao diện của công cụ sử dụng cho bài thực hành này.

Khi đăng nhập thành công, vào tab administrator, feed status, khi tất cả đều đang ở trạng thái current, công cụ đã sẵn sàng.



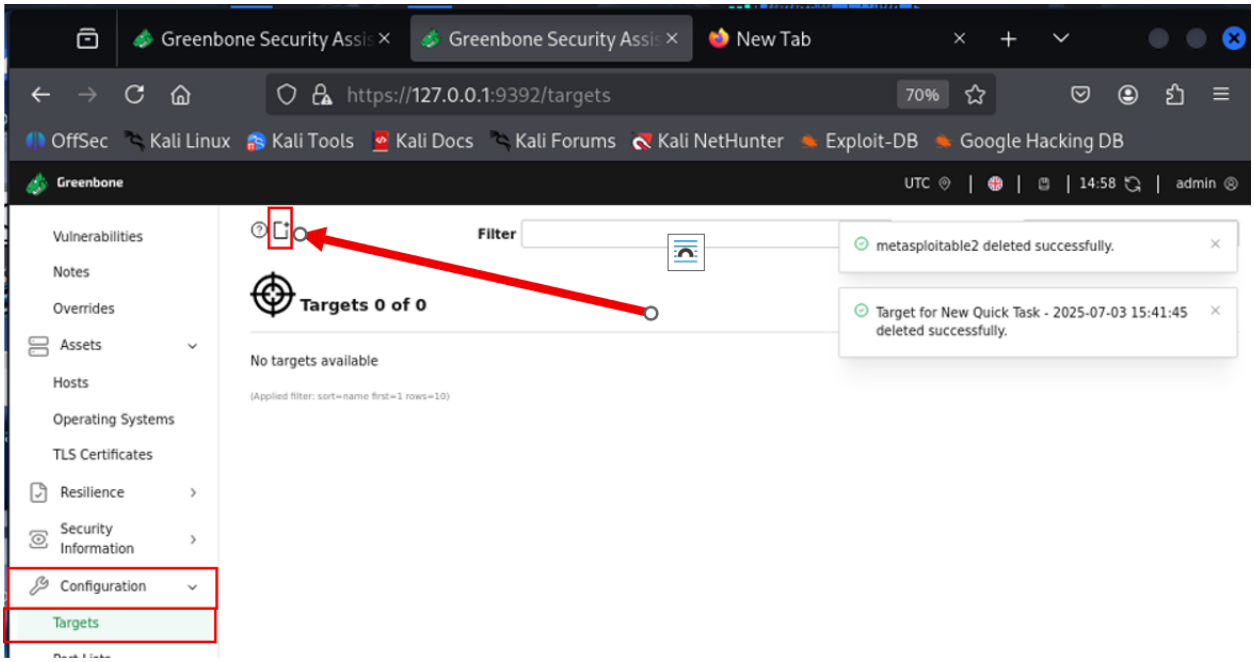
Trên máy metasploitable2, dùng tài khoản mật khẩu msfadmin/msfadmin để đăng nhập, sau đó chạy lệnh ifconfig để kiểm tra ip.



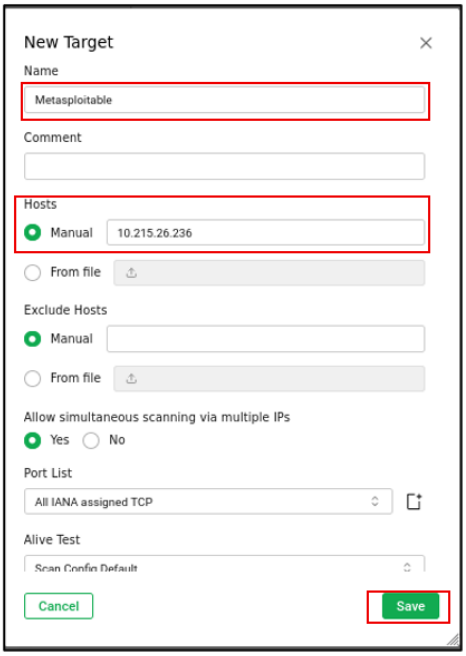
Trên browser của kali, vào địa chỉ IP của metasploitable2, sau đó web sẽ có giao diện như ảnh ở dưới, như vậy phần chuẩn bị lab đã xong.

1. Tạo mục tiêu để quét.

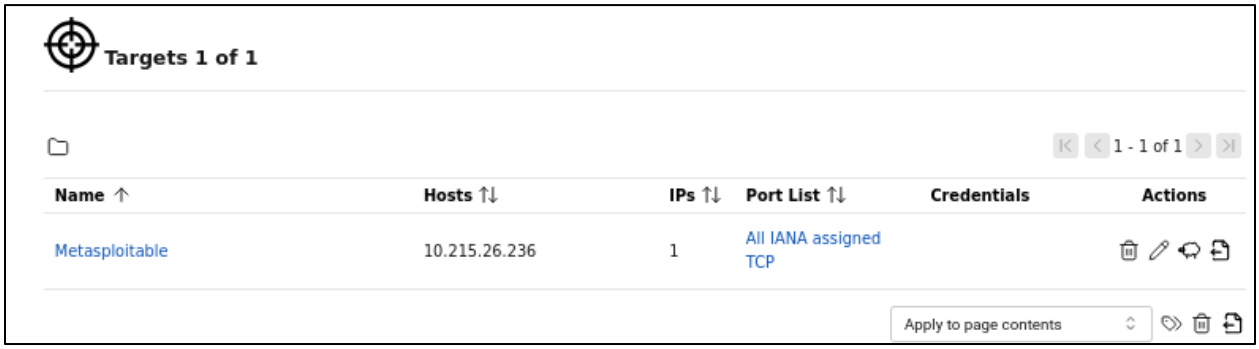
Ở thanh bên trái, Chọn Configuration→Targets, sau đó ấn vào biểu tượng file có dấu cộng.



Sau đó, một cửa sổ sẽ xuất hiện, chúng ta sẽ cần điền vào thông tin Name(tên của mục tiêu) và host(địa chỉ ip của mục tiêu), sau đó nhấn Save để lưu.

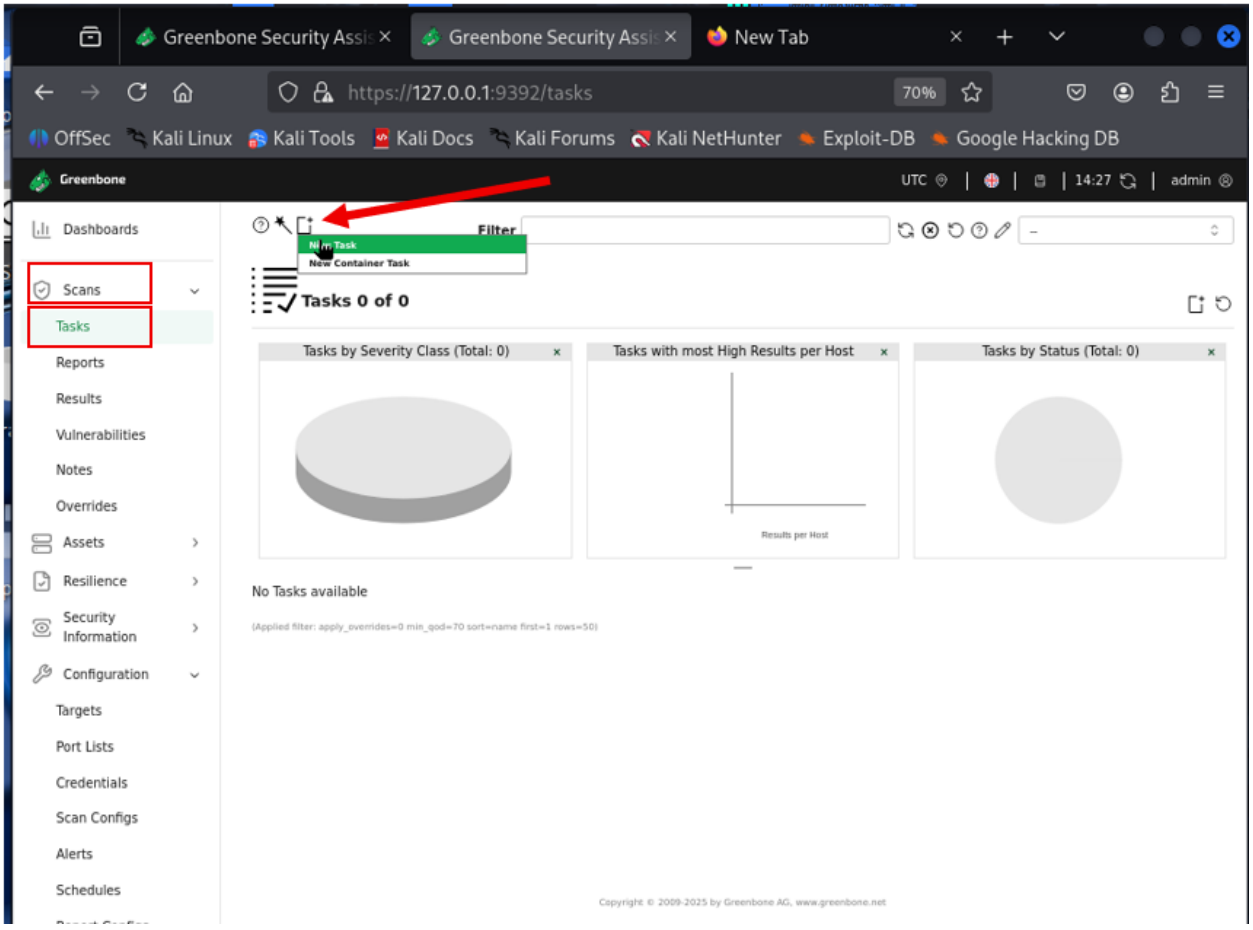


➔ Như vậy, chúng ta đã thành công tạo một mục tiêu để quét.

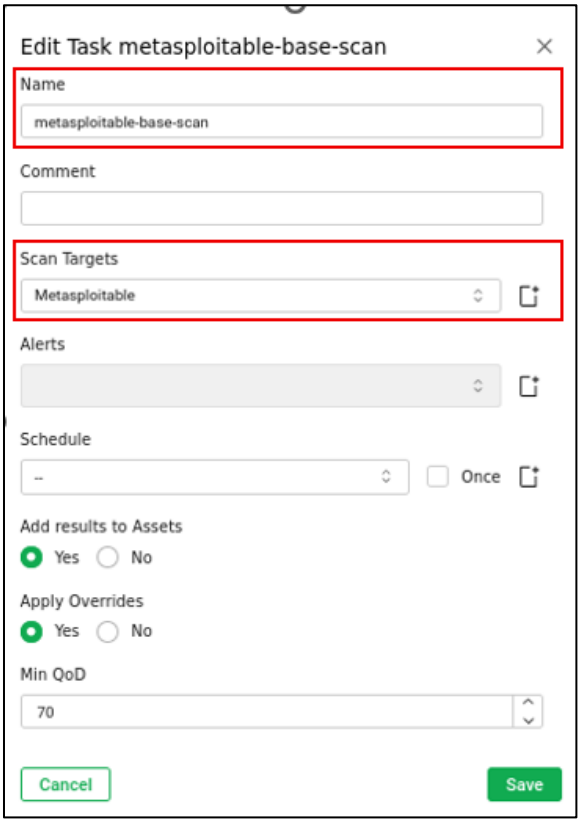


2. Tạo task để quét.

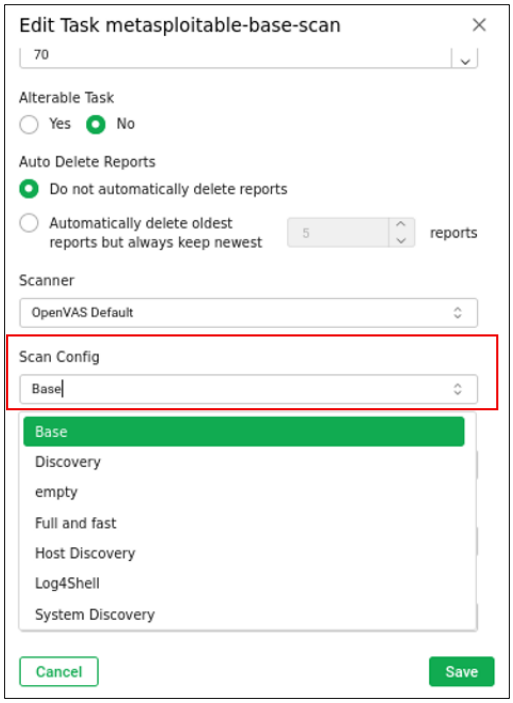
Ở mục Scans chọn Task, ấn vào biểu tượng thư mục có dấu cộng, sau đó chọn New Task.



Lúc này sẽ có một cửa sổ hiện lên, đặt tên và target để scan.



Cuộn chuột xuống dưới ở tab scan-config, click vào để xem các kiểu scan hiện có.

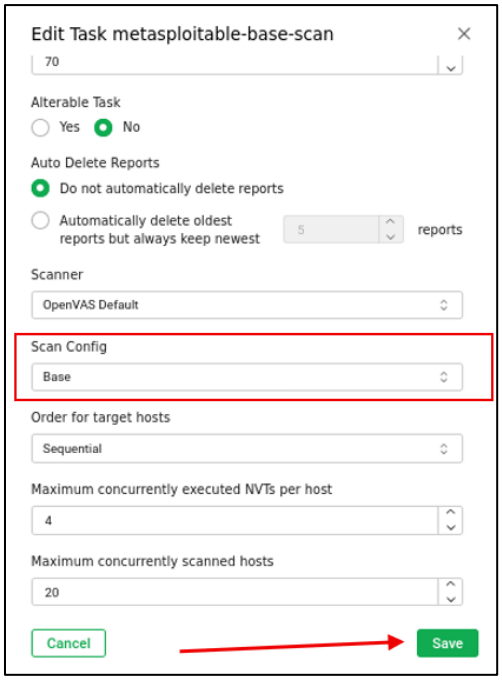


Như hình đã thấy gồm có 7 kiểu scan, dưới đây là bảng chức năng của từng kiểu scan.

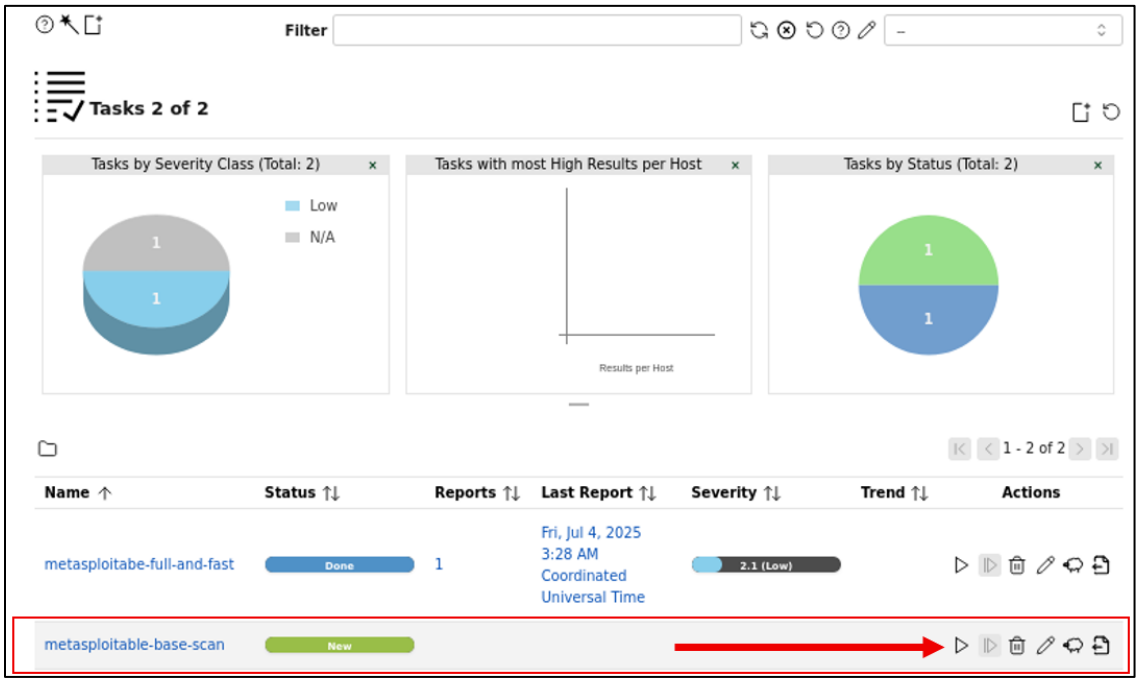
Chú thích: NVT là Network Vulnerability Test

Scan Config	**Mục đích chính**	**Phạm vi kiểm tra**	**Đặc điểm**
Empty	Khởi tạo cấu hình trống, chỉ chứa phần khung cơ bản	Không có NVT nào được chạy	Dùng để tự xây dựng kịch bản quét tùy chỉnh từ đầu, không tốn tài nguyên ban đầu
Base	Cơ sở để mở rộng, chạy các bài test nền tảng	Một tập nhỏ các NVT cơ bản (không đầy đủ)	Nhanh, ít tiêu thụ tài nguyên, thường chỉ dùng làm tham khảo
Discovery	Khám phá host, port, dịch vụ đang mở	Thực hiện ping/TCP connect đến port phổ biến, banner grab	Không kiểm thử lỗ hổng sâu, dùng để map sơ bộ hạ tầng
Host Discovery	Chỉ xác định xem host còn sống và port nào mở	ICMP ping, TCP/UDP ping đến các port xác định	Rất nhanh, không phát hiện lỗ hổng, chỉ "đánh dấu" host/port
System Discovery	Thăm dò chi tiết thông tin hệ thống	OS fingerprinting, banner grab, version detection	Giúp nắm OS, dịch vụ, version, không khai thác lỗ hổng
Full and fast	Quét toàn diện với tốc độ tương đối nhanh	Toàn bộ NVT "Full and fast" feed (hơn 50.000 test)	Cân bằng giữa phủ rộng và thời gian quét Thường dùng chính
Log4Shell	Chuyên biệt phát hiện lỗ hổng Log4Shell (CVE-2021-44228)	Chạy các NVT liên quan đến Log4j 2 (RCE qua JNDI lookup)	Rất nhanh, tập trung duy nhất vào một CVE Dùng để validate gói vá

Với lần scan này chúng ta sẽ bắt đầu với Base-scan, chọn Base, sau đó nhấn save

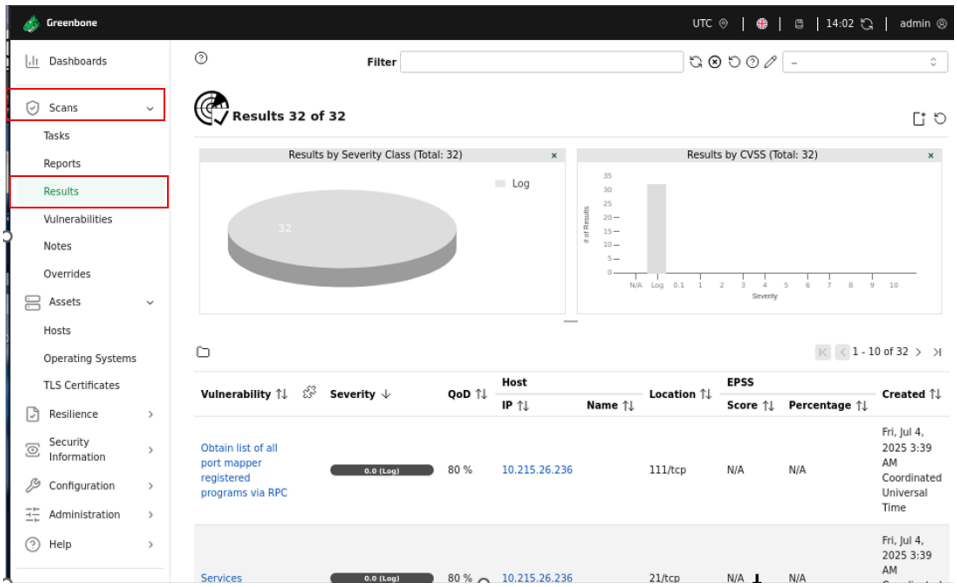


Task được tạo sẽ giống hình bên dưới. Sau đó, nhấn biểu tượng tam giác để bắt đầu quét.

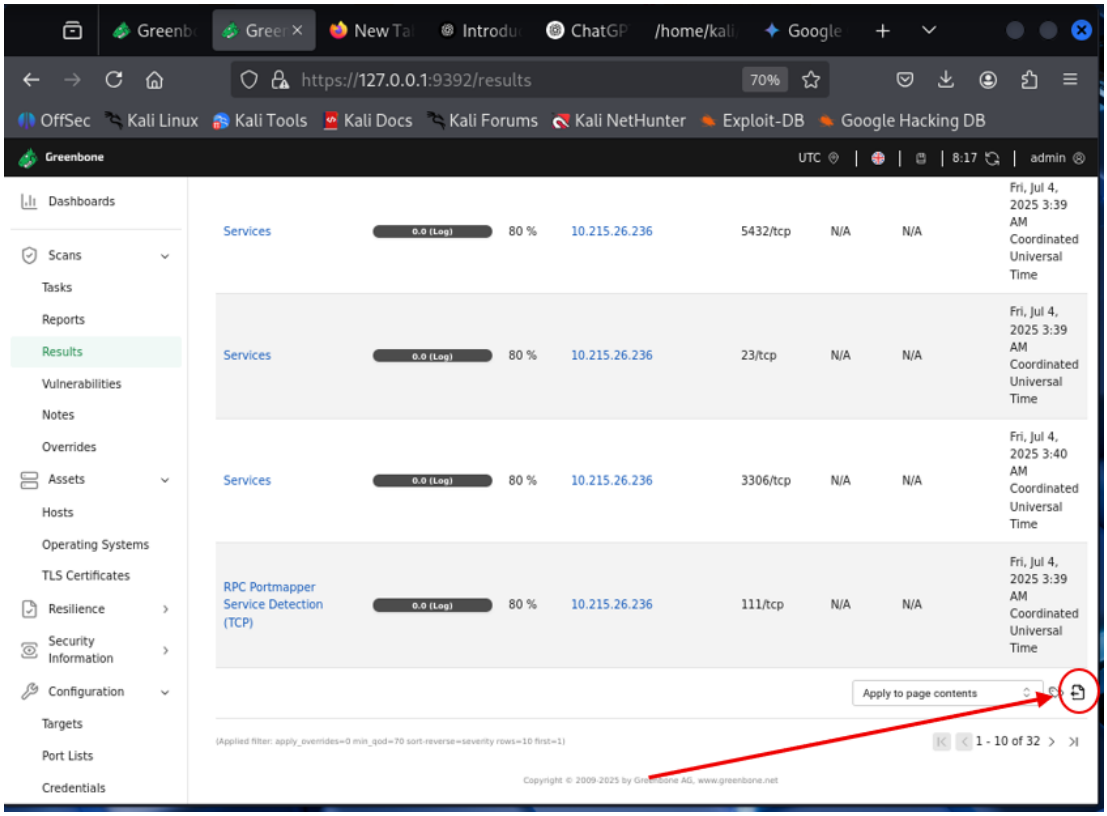


Sau khi scan xong

Để xem kết quả sau khi scan, chúng ta sẽ truy cập vào Scans→Results, ở đây chứa toàn bộ thông tin đã scan được từ tất cả các task.

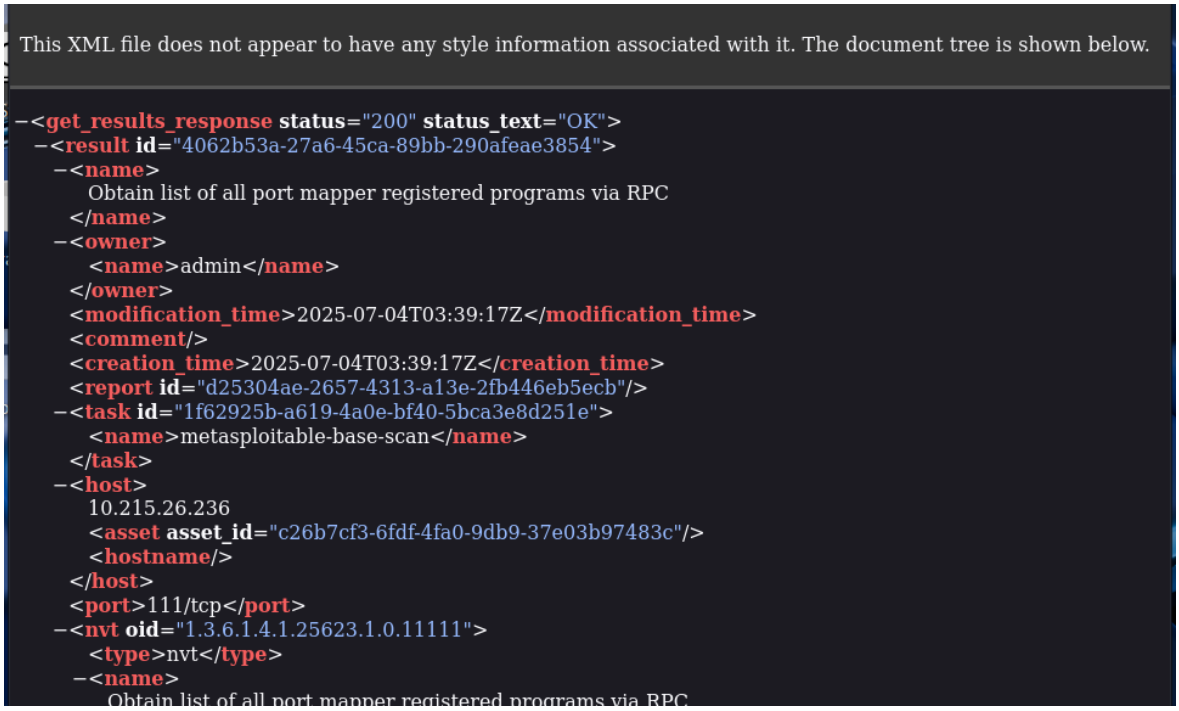


Để dễ dàng phân tích kết quả đạt được, chúng ta có thể xuất kết quả ra file XML, sau đó nhờ AI phân tích các kết quả thu được, nhấn vào biểu tượng bên dưới.

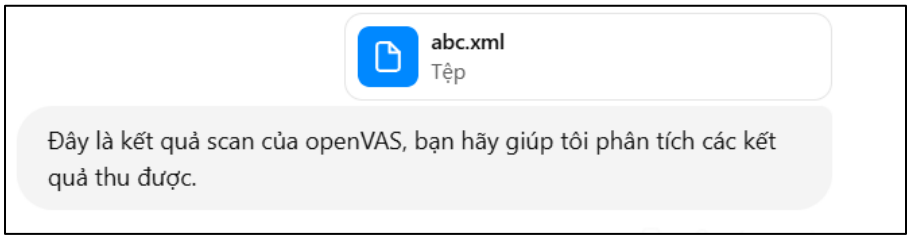


File kết quả sẽ được tải về như hình bên dưới.

Nhấn vào sẽ có dạng như sau.



Coppy toàn bộ nội dung (hoặc gửi file) lên con chatboxAI bất kì, AI sẽ hỗ trợ chúng ta phân tích kết quả thu được. Giúp chúng ta dễ dàng nắm được thông tin và không bỏ xót bất kì lỗ hổng nào. Ví dụ ở đây chúng ta sử dụng chatGPT.



ChatGPT dễ dàng phân tích và tổng kết từ kết quả như hình bên dưới.

Cổng	Dịch vụ	Thông tin chi tiết
21/tcp	FTP (vsFTPd 2.3.4)	Dịch vụ FTP có thể dễ bị tấn công, đặc biệt nếu không cấu hình giới hạn quyền người dùng.
22/tcp	SSH	Dịch vụ cho phép kết nối từ xa; cần chú ý đến chính sách xác thực và cấu hình bảo mật.
23/tcp	Telnet	Dịch vụ này truyền dữ liệu dưới dạng **cleartext**, tiềm ẩn **rủi ro cao** nếu được sử dụng trên mạng mở.
25/tcp	SMTP (Postfix - ESMTP)	Máy chủ gửi email; cần kiểm tra cấu hình relay và xác thực để tránh bị lợi dụng spam.
80/tcp	Web Server	Có dịch vụ HTTP đang hoạt động. Không rõ là Apache hay loại nào, cần quét sâu hơn.
111/tcp	RPC Portmapper	Dịch vụ quản lý ánh xạ RPC; thường thấy trong hệ thống UNIX/Linux, nhưng nếu lộ ra mạng công cộng thì **rất nguy hiểm**.
2121/tcp	FTP (ProFTPD 1.3.1)	Dịch vụ FTP thứ hai; có thể đang dùng cho mục đích khác biệt, nhưng **nên cấu hình rõ ràng** phân quyền.
3306/tcp	MySQL (không xác định rõ banner)	Cổng mặc định của MySQL. Nếu không bảo vệ bằng mật khẩu mạnh hoặc tường lửa, dễ bị dò quét brute-force.
5432/tcp	PostgreSQL (không xác định rõ)	Cổng mặc định của PostgreSQL; nếu không bảo vệ kỹ, có thể dẫn đến rò rỉ dữ liệu.

Đây là link của chatGPT chứa đáp án cho bạn dễ dàng tham khảo: giữ ctrl và ấn vào đây!

Như vậy chúng ta đã thực hiện xong base-scan. Để thực hành thêm, các bạn hãy thực hiện trên các kiểu scan khác nhé!!!