

## Lab Scanning with OpenVas

### Chuẩn bị

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

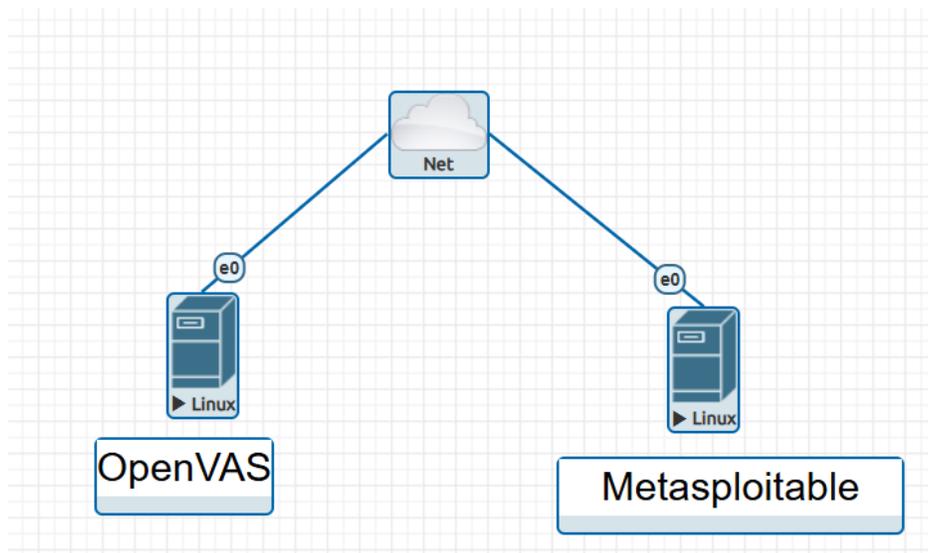
### Mục tiêu

- 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`.

```
root@kali: ~
File Actions Edit View Help
[>] You can now run gvm-check-setup to make sure everything is correctly configured

(root@kali)-[~]
#
# gvm-check-setup
gvm-check-setup 25.04.0
This script is provided and maintained by Debian and Kali.
Test completeness and readiness of GVM-25.04.0
Step 1: Checking OpenVAS (Scanner)...
OK: OpenVAS Scanner is present in version 23.19.0.
OK: Notus Scanner is present in version 22.6.5.
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/gnupg/*
OK: _gvm owns all files in /var/lib/openvas/gnupg
OK: redis-server is present.
OK: scanner (db_address setting) is configured properly using the redis-server socket: /var/run/redis-openvas/redis-server.sock
OK: the mqtt_server_uri is defined in /etc/openvas/openvas.conf
OK: _gvm owns all files in /var/lib/openvas/plugins
OK: NVT collection in /var/lib/openvas/plugins contains 94095 NVTs.
OK: The notus directory /var/lib/notus/products contains 501 NVTs.
Checking that the obsolete redis database has been removed
Could not connect to Redis at /var/run/redis-openvas/redis-server.sock: No such file or directory
```

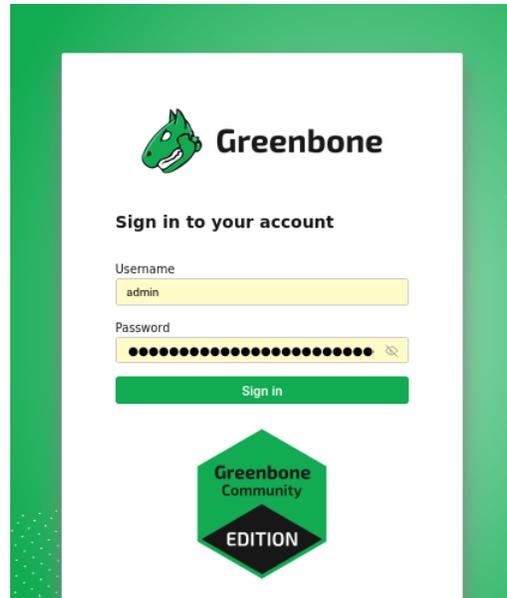
Chạy lệnh `gvm-start`

```
root@kali: ~
File Actions Edit View Help
Starting gvmd service
Waiting for gvmd service
OK: gvmd service is active.
Starting gsad service
Waiting for gsad service
OK: gsad service is active.
Step 8: Checking few other requirements...
OK: nmap is present.
OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
OK: nsis found, LSC credential package generation for Microsoft Windows targets is likely to work.
OK: xsltproc found.
WARNING: Your password policy is empty.
SUGGEST: Edit the /etc/gvm/pwpolicy.conf file to set a password policy.
Step 9: Checking greenbone-security-assistant...
OK: greenbone-security-assistant is installed
It seems like your GVM-25.04.0 installation is OK.

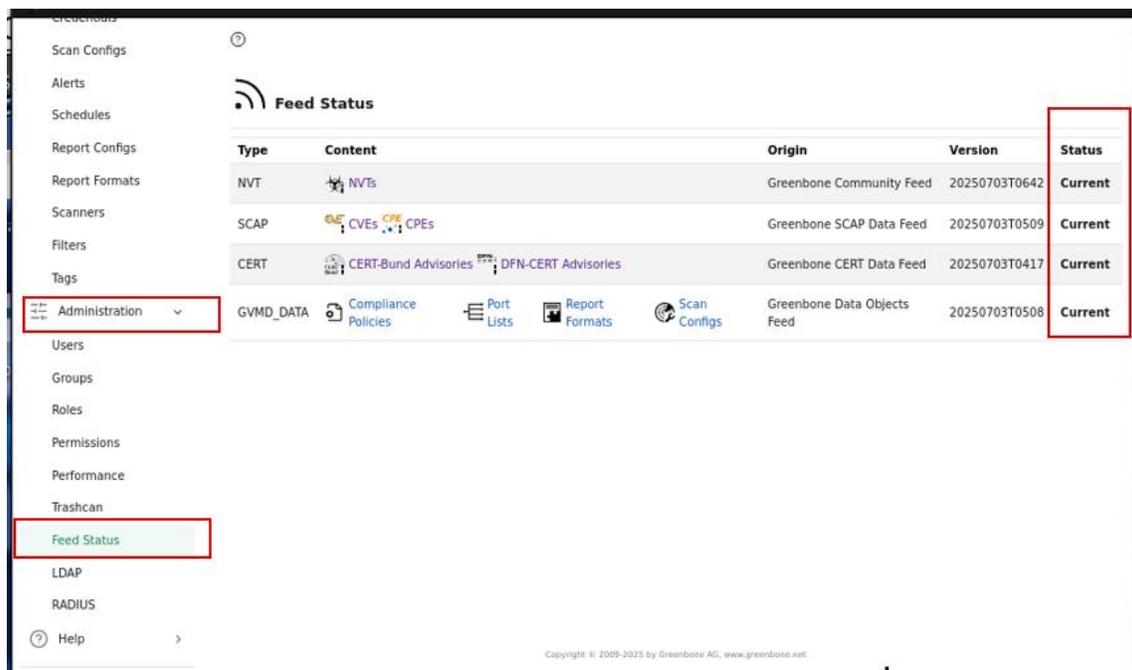
(root@kali)-[~]
# gvm-start
[i] GVM services are already running

(root@kali)-[~]
#
```

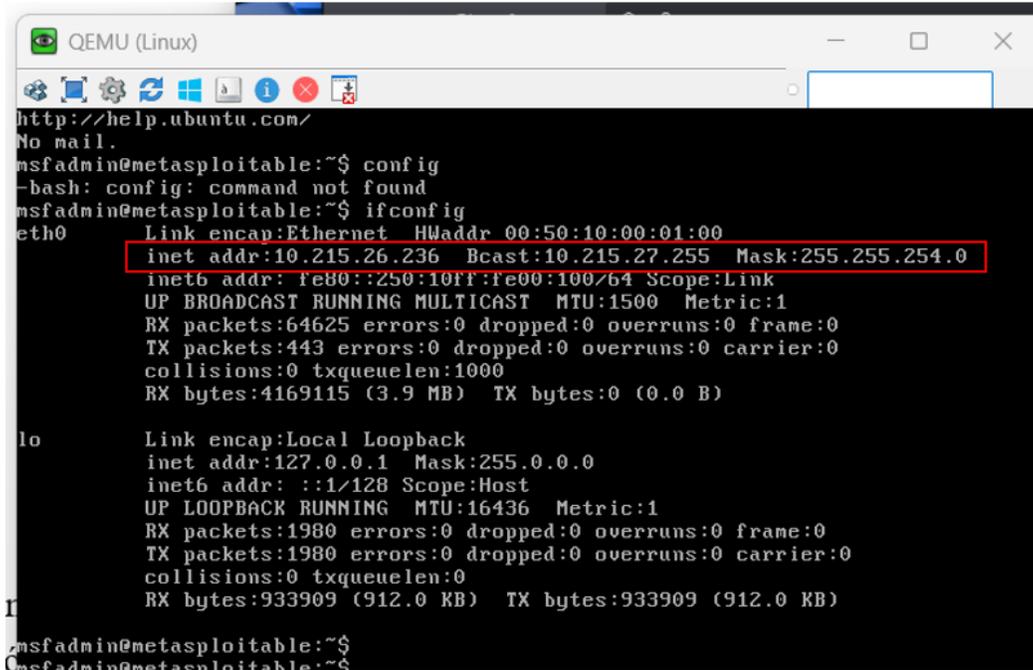
Sau đó sẽ có một trang web xuất hiện, sử dụng tài khoản admin để đăng nhập. Đây là giao diện của công cụ sử dụng cho bài thực hành này.



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.



```
QEMU (Linux)
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ config
-bash: config: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:10:00:01:00
          inet addr:10.215.26.236  Bcast:10.215.27.255  Mask:255.255.254.0
          inet6 addr: fe80::250:10ff:fe00:100/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:64625 errors:0 dropped:0 overruns:0 frame:0
          TX packets:443 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4169115 (3.9 MB)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1980 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1980 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:933909 (912.0 KB)  TX bytes:933909 (912.0 KB)

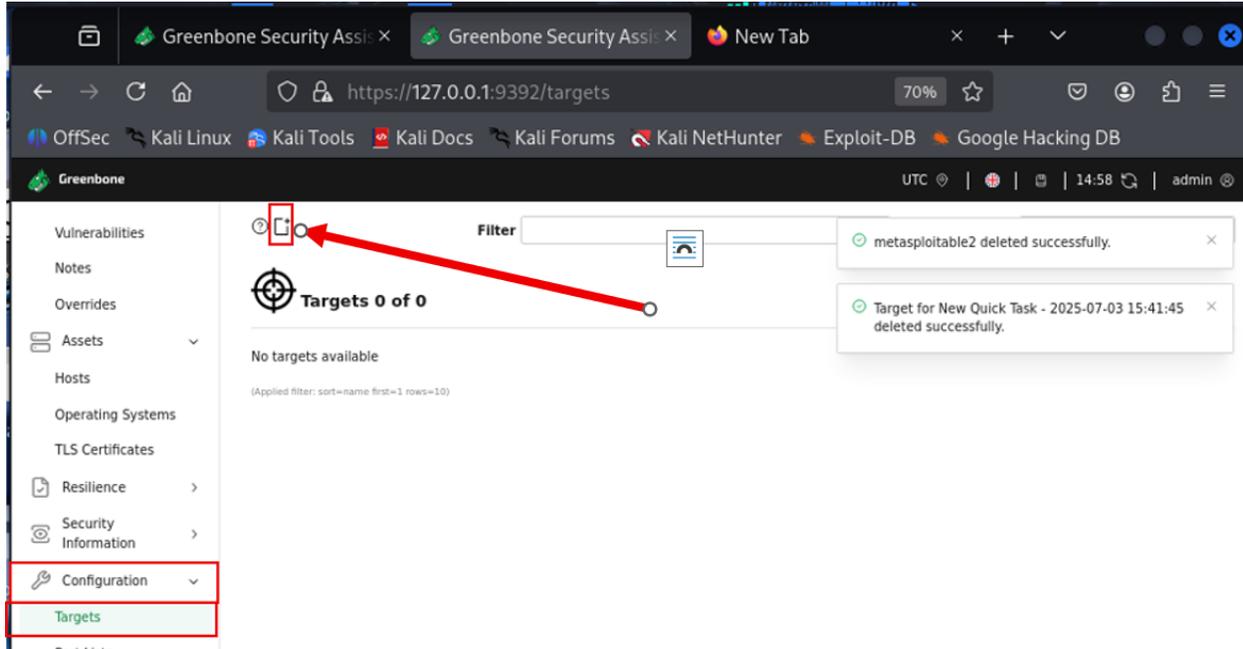
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
```

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.

New Target

Name  
Metasploitable

Comment

Hosts  
 Manual 10.215.26.236  
 From file

Exclude Hosts  
 Manual  
 From file

Allow simultaneous scanning via multiple IPs  
 Yes  No

Port List  
All IANA assigned TCP

Alive Test  
Scan Confir Default

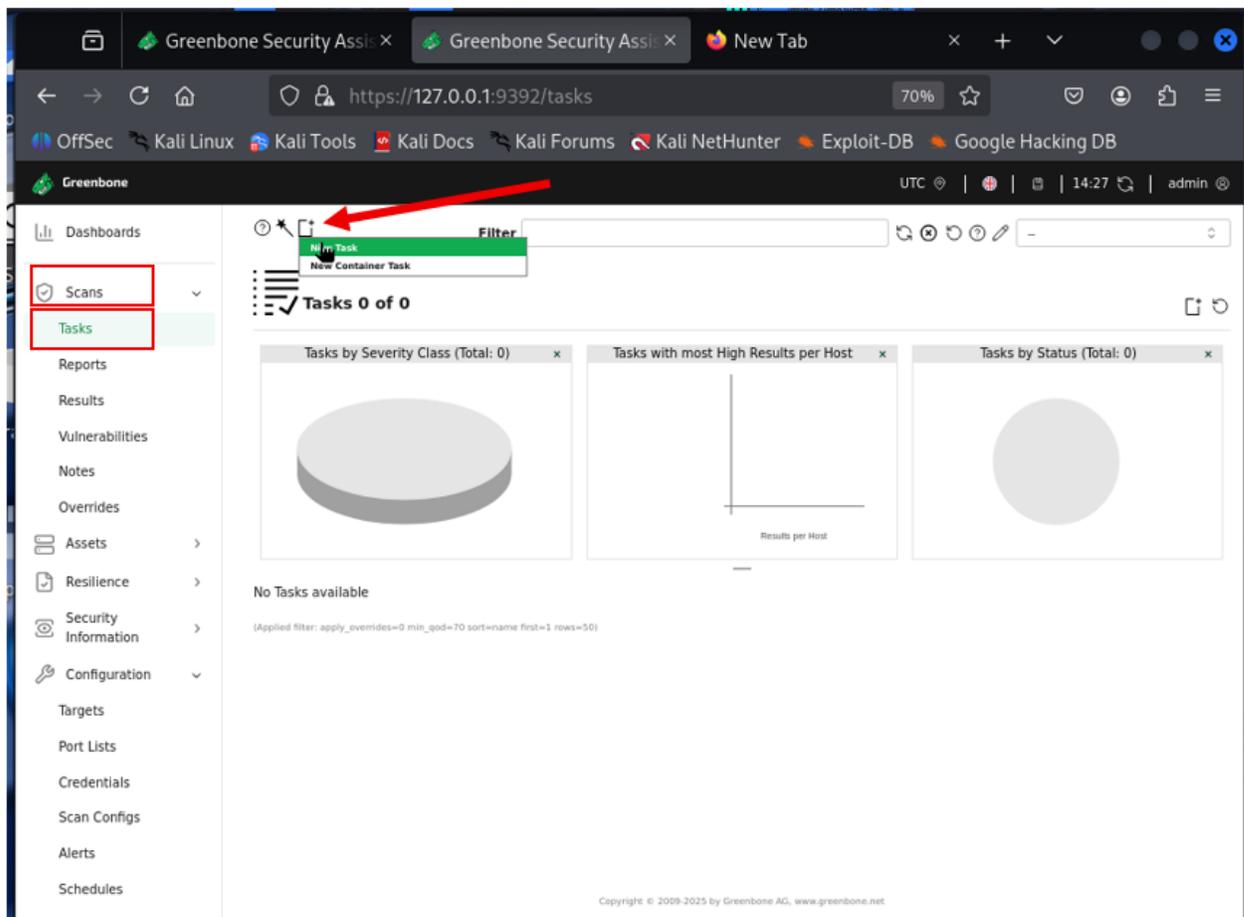
Cancel Save

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

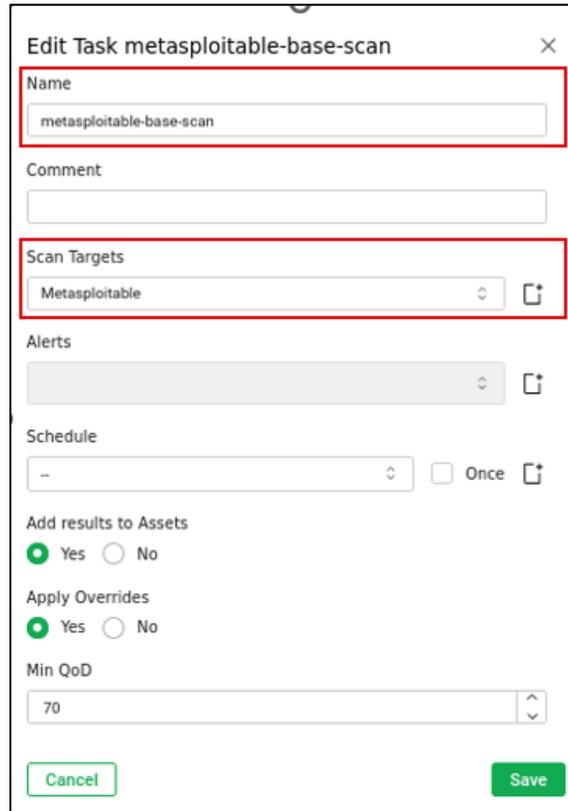
Name ↑	Hosts ↓	IPs ↓	Port List ↓	Credentials	Actions
Metasploitable	10.215.26.236	1	All IANA assigned TCP		

## 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.



**Edit Task metasploitable-base-scan**

Name  
metasploitable-base-scan

Comment

Scan Targets  
Metasploitable

Alerts

Schedule  
--

Once

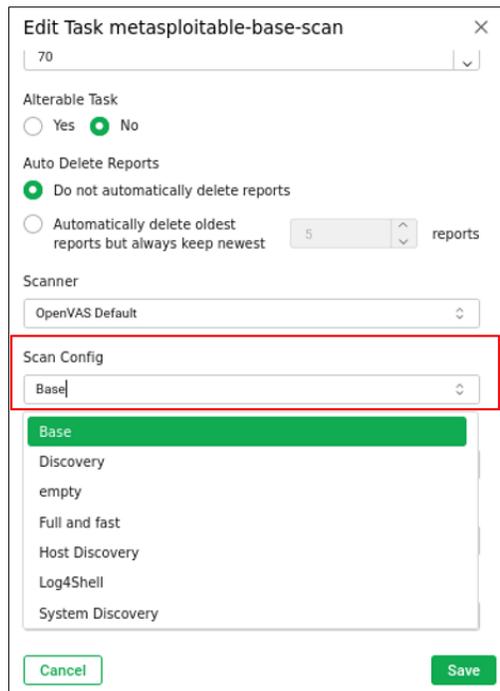
Add results to Assets  
 Yes  No

Apply Overrides  
 Yes  No

Min QoD  
70

Cancel Save

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



**Edit Task metasploitable-base-scan**

70

Alterable Task  
 Yes  No

Auto Delete Reports  
 Do not automatically delete reports  
 Automatically delete oldest reports but always keep newest 5 reports

Scanner  
OpenVAS Default

Scan Config  
Base

Base  
Discovery  
empty  
Full and fast  
Host Discovery  
Log4Shell  
System Discovery

Cancel Save

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
<b>Empty</b>	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
<b>Base</b>	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
<b>Discovery</b>	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
<b>Host Discovery</b>	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
<b>System Discovery</b>	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
<b>Full and fast</b>	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
<b>Log4Shell</b>	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 và

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

Edit Task metasploitable-base-scan

70

Alterable Task  
 Yes  No

Auto Delete Reports  
 Do not automatically delete reports  
 Automatically delete oldest reports but always keep newest 5 reports

Scanner  
OpenVAS Default

Scan Config  
Base

Order for target hosts  
Sequential

Maximum concurrently executed NVTs per host  
4

Maximum concurrently scanned hosts  
20

Cancel Save

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

Filter

Tasks 2 of 2

Tasks by Severity Class (Total: 2)

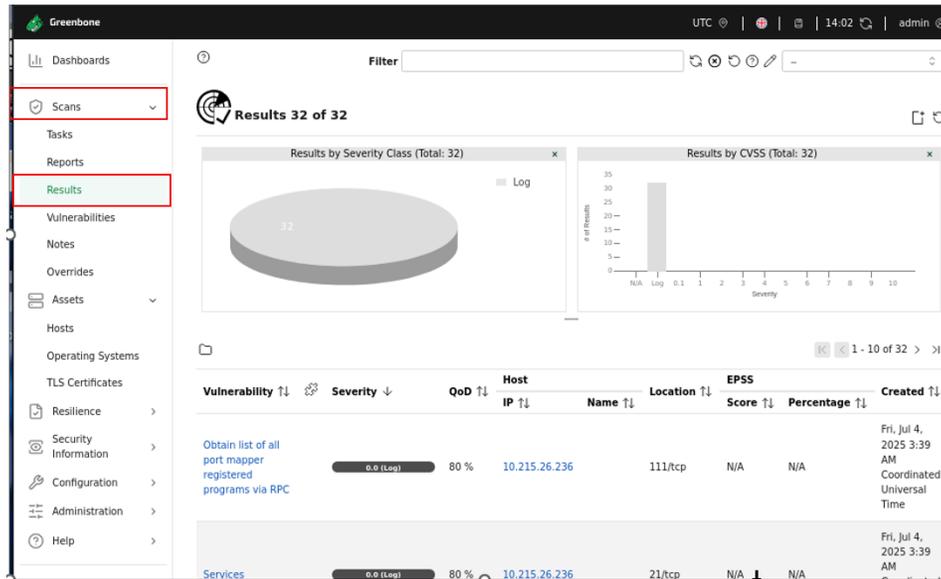
Tasks with most High Results per Host

Tasks by Status (Total: 2)

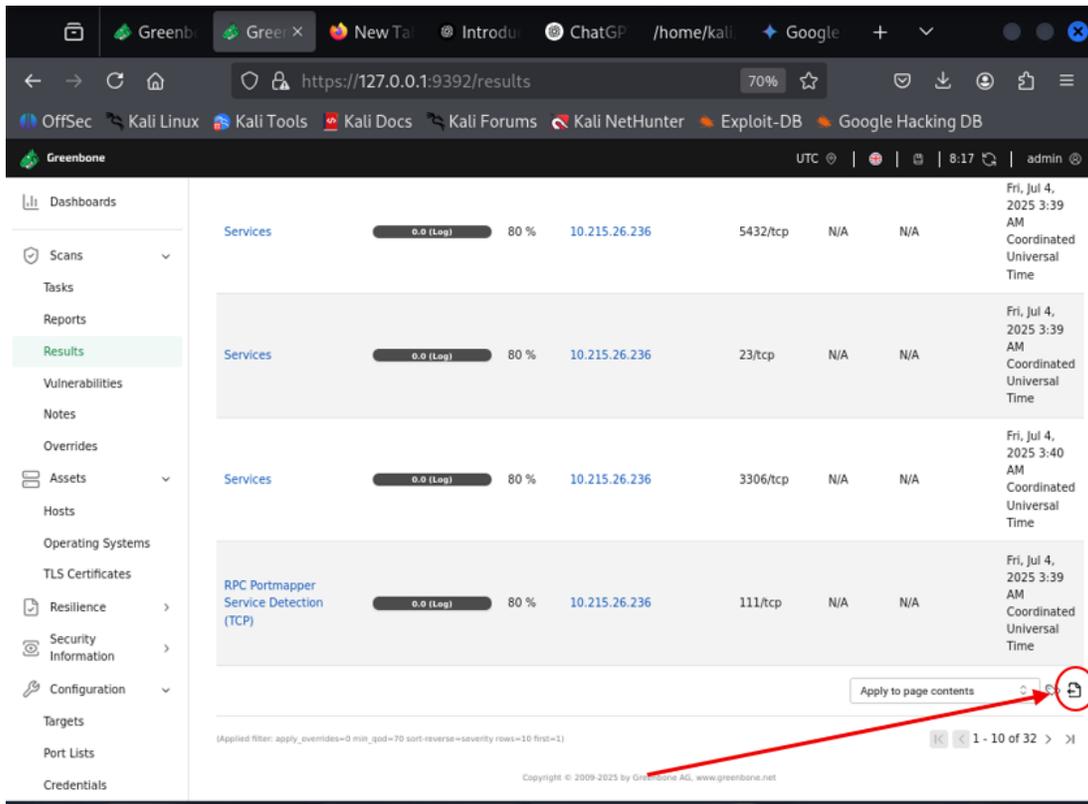
Name ↑	Status ↑↓	Reports ↑↓	Last Report ↑↓	Severity ↑↓	Trend ↑↓	Actions
metasploitabe-full-and-fast	Done	1	Fri, Jul 4, 2025 3:28 AM Coordinated Universal Time	2.1 (Low)		
metasploitable-base-scan	New					

Sau khi scan xong

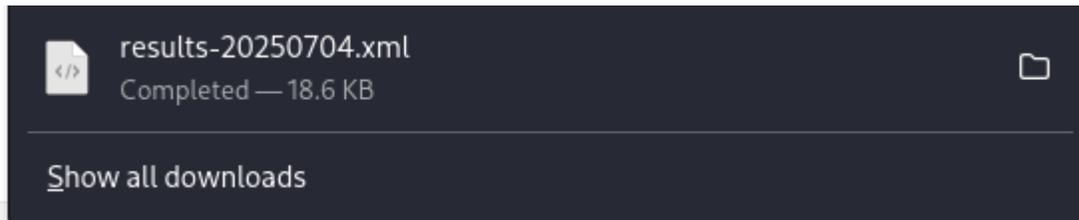
Để xem kết quả sau khi scan, chúng ta sẽ truy cập vào Scans → Results, ở đây chứa toàn bộ thông tin đã scan được từ tất cả các task.



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.

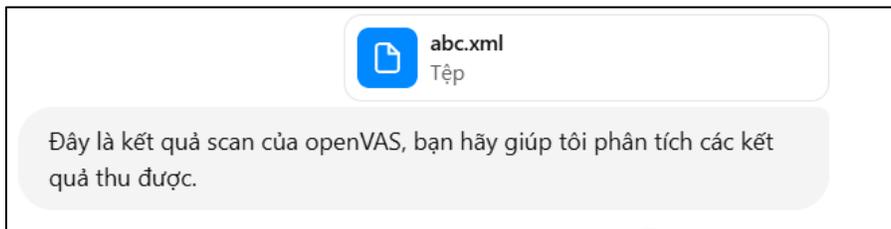


Nhấn vào sẽ có dạng như sau.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
-<get_results_response status="200" status_text="OK">
-<result id="4062b53a-27a6-45ca-89bb-290afeae3854">
  -<name>
    Obtain list of all port mapper registered programs via RPC
  </name>
  -<owner>
    <name>admin</name>
  </owner>
  <modification_time>2025-07-04T03:39:17Z</modification_time>
  <comment/>
  <creation_time>2025-07-04T03:39:17Z</creation_time>
  <report id="d25304ae-2657-4313-a13e-2fb446eb5ecb"/>
  -<task id="1f62925b-a619-4a0e-bf40-5bca3e8d251e">
    <name>metasploitable-base-scan</name>
  </task>
  -<host>
    10.215.26.236
    <asset asset_id="c26b7cf3-6fdf-4fa0-9db9-37e03b97483c"/>
    <hostname/>
  </host>
  <port>111/tcp</port>
  -<nvt oid="1.3.6.1.4.1.25623.1.0.11111">
    <type>nvt</type>
  </nvt>
  -<name>
    Obtain list of all port mapper registered programs via RPC
```

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 sót 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 <b>cleartext</b> , 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 <b>rất nguy hiểm</b> .
2121/tcp	FTP (ProFTPD 1.3.1)	Dịch vụ FTP thứ hai; có thể đang dùng cho mục đích khác biệt, nhưng <b>nhớ cấu hình rõ ràng</b> 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 để 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!!!