Bài: 5.2 Thực nghiệm Quét lỗ hổng bằng Nessus Vulnerability Scanning Tool

Xem bài học trên website để ủng hộ Kteam: 5.2 Thực nghiệm Quét lỗ hổng bằng Nessus Vulnerability Scanning Tool

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

Thực nghiệm Quét lỗ hổng bằng Nessus Vulnerability Scanning Tool

Case study

Trong nghiên cứu này, chúng ta sẽ sử dụng công cụ quét lỗ hổng bảo mật để quét một mạng riêng **10.10.10.0/24**. Thực nghiệm này được thực hiện trên máy ảo có hệ điều hành Windows 10 với công cụ là Nessus vulnerability scanning tool. Bạn có thể tải xuống công cụ này từ website của Tenable:

> https://www.tenable.com/products/nessus/nessus-professional

Configuration

1. Tải xuống và cài đặt **Nessus vulnerability scanning tool**.
2. Mở một web browser.
3. Đến URL http://localhost:8834

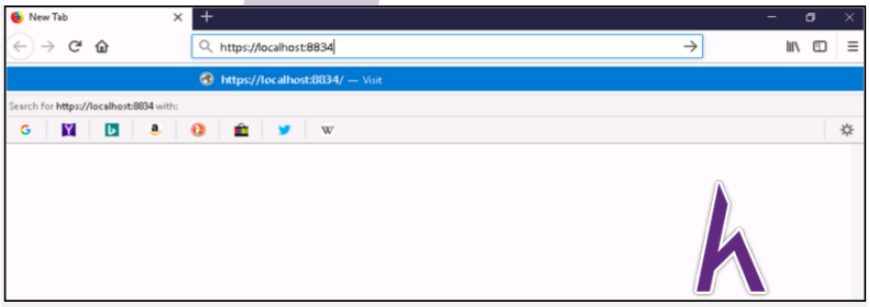

Figure 5-08 https://localhost:8834

4. Click vào nút **Advanced**.

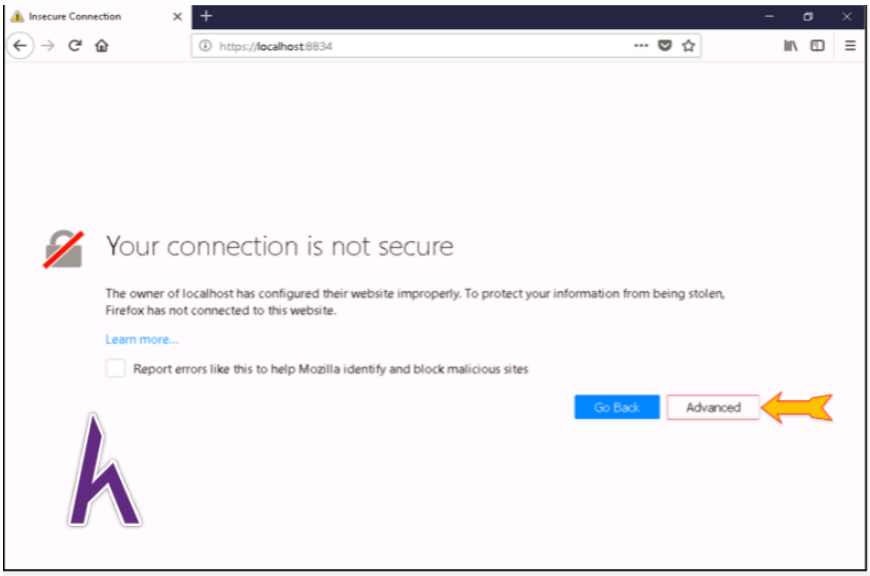

Figure 5-09 Security Exception required

5. Tiếp tục click vào **Add Security Exception**.

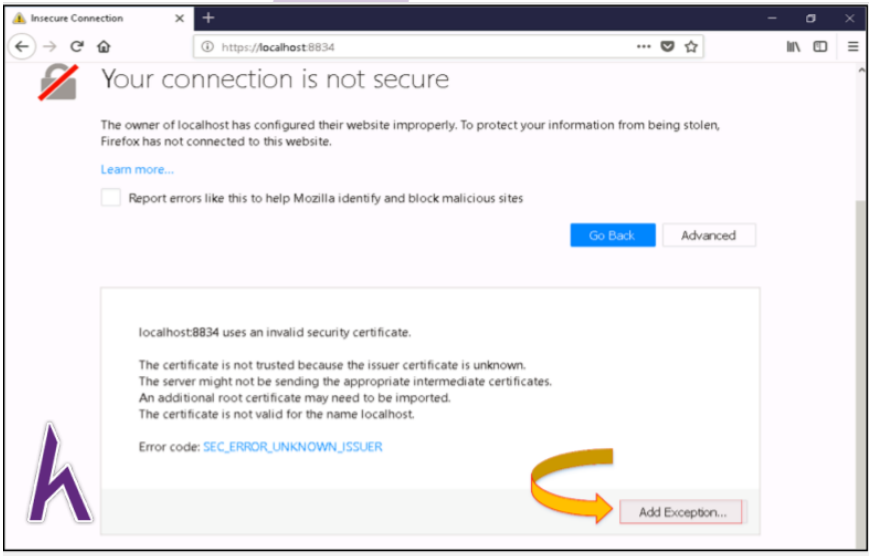

Figure 5-10 Add Security Exception

6. Click vào **Confirm Security Exception**.

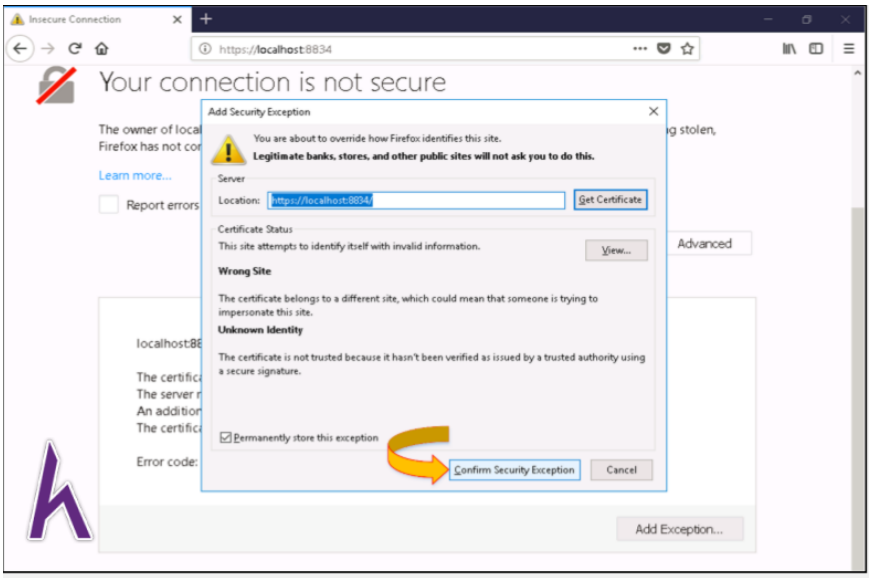

Figure 5-11 Confirm Security Exception

7. Nhập **Username** và **Password** tài khoản Nessus của bạn. (Phải đăng kí một tài khoản để tải công cụ từ website).

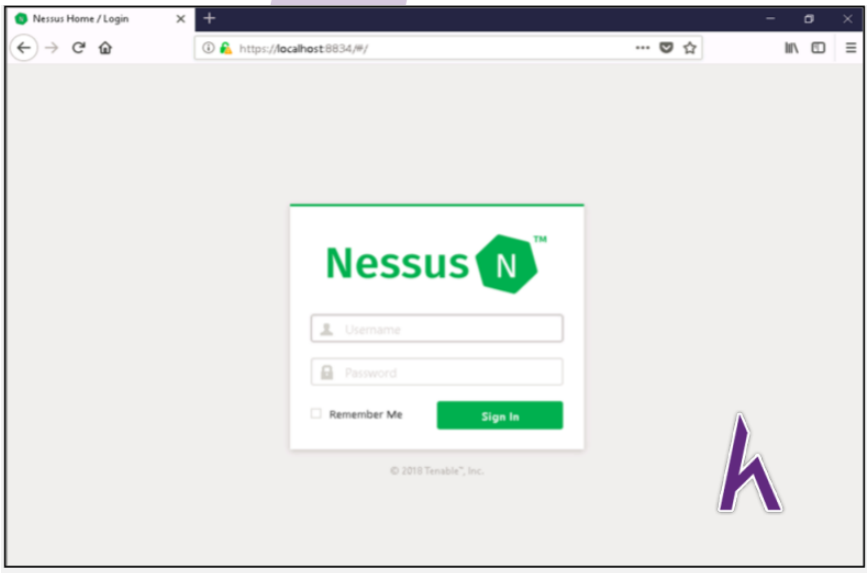

Figure 5-12 Nessus Login Page

8. **Dashboard** dưới đây sẽ hiện ra.

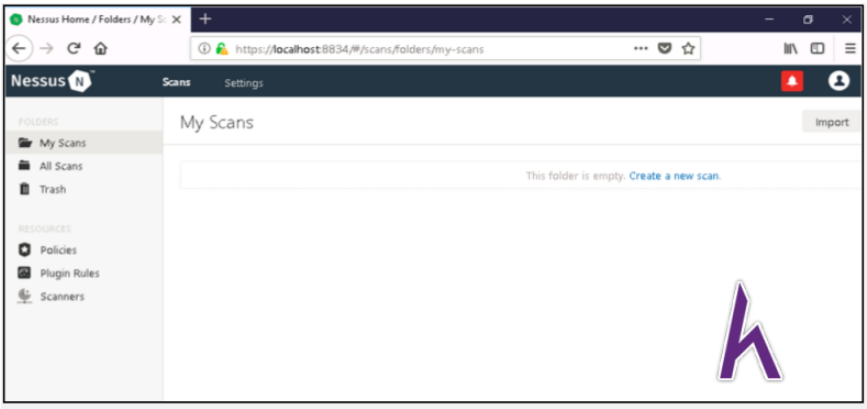

Figure 5-13 Nessus Dashboard

9. Mở tab **Policies** và click vào **Create New Policy**.

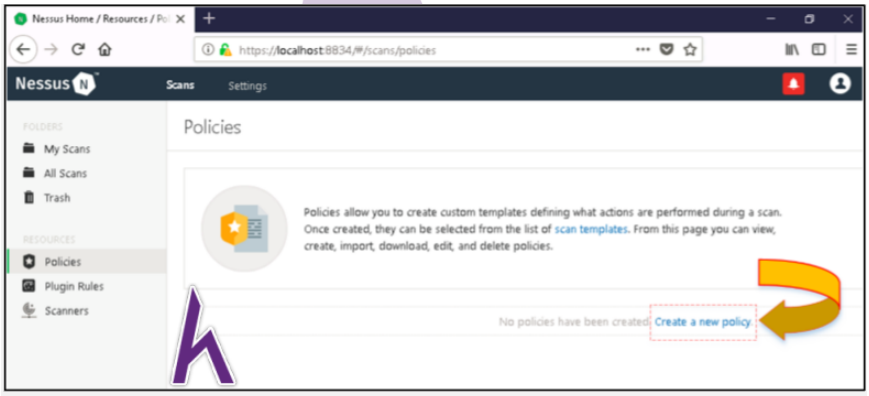

Figure 5-14 Create new policy

10. Trong phần **Basic Setting**, đặt tên cho **Policy**.

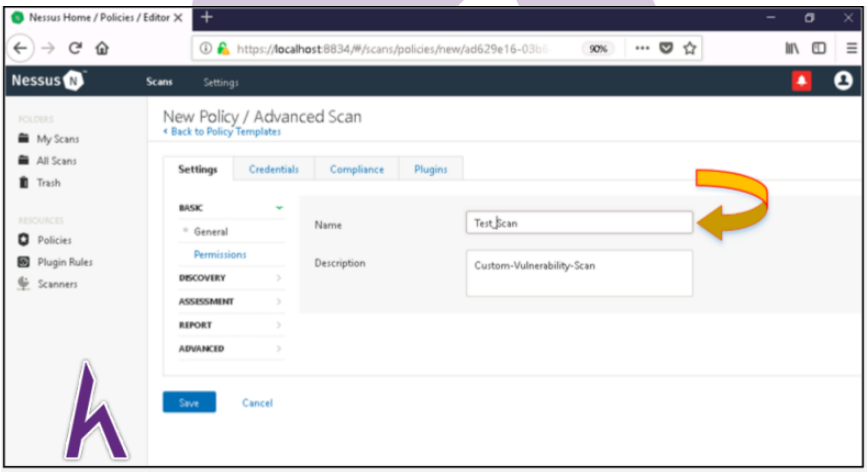

Figure 5-15 Configuring Policy

11. Trong phần **Settings** > **basics** > **Discovery**, **configure Discovery settings**.

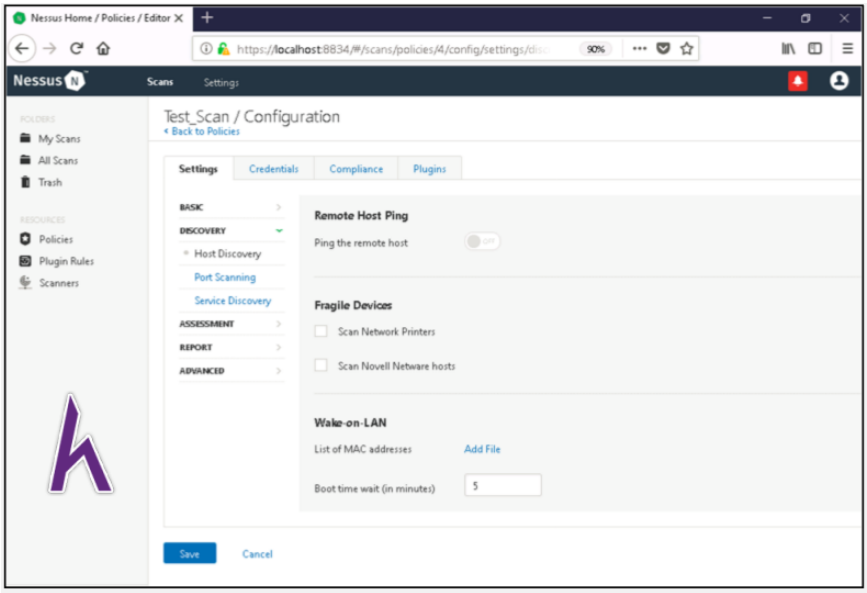

Figure 5-16 Configuring Policy

12. **Configure Port Scanning Settings** trong **Port Scanning Tab**.

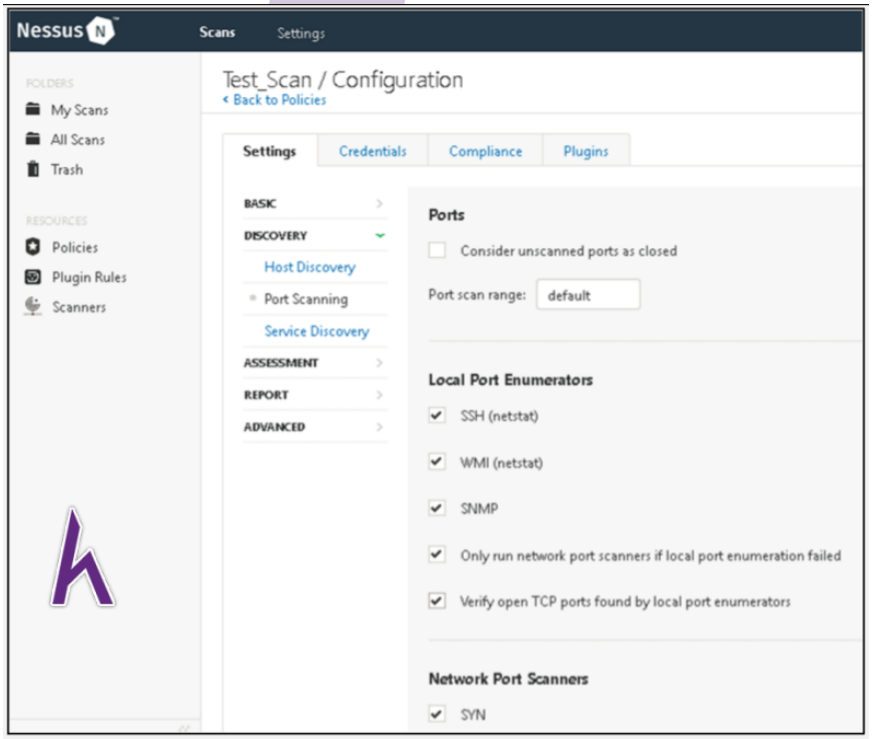

Figure 5-17 Configuring Policy

13. Trong **Report tab**, **configured settings** như yêu cầu.

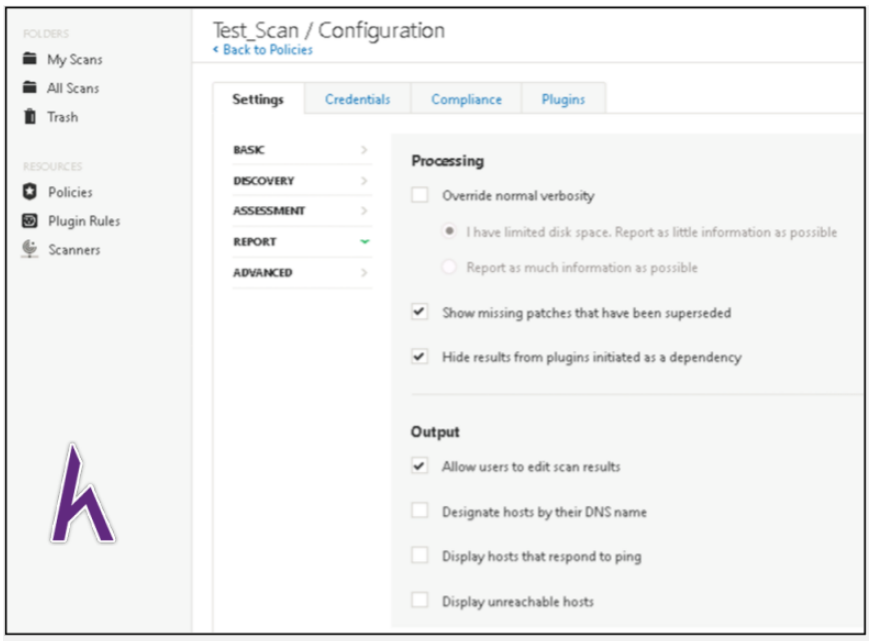

Figure 5-18 Configuring Policy

14. Trong **Advanced tab**, configure parameters:

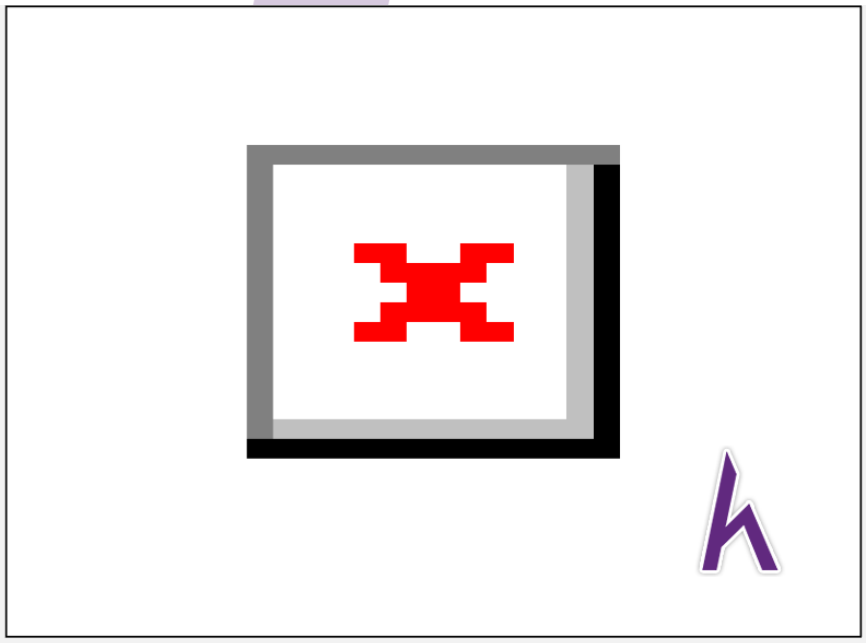

Figure 5-19 Configuring Policy

15. Đến **Credentials tab** để cài đặt credentials.

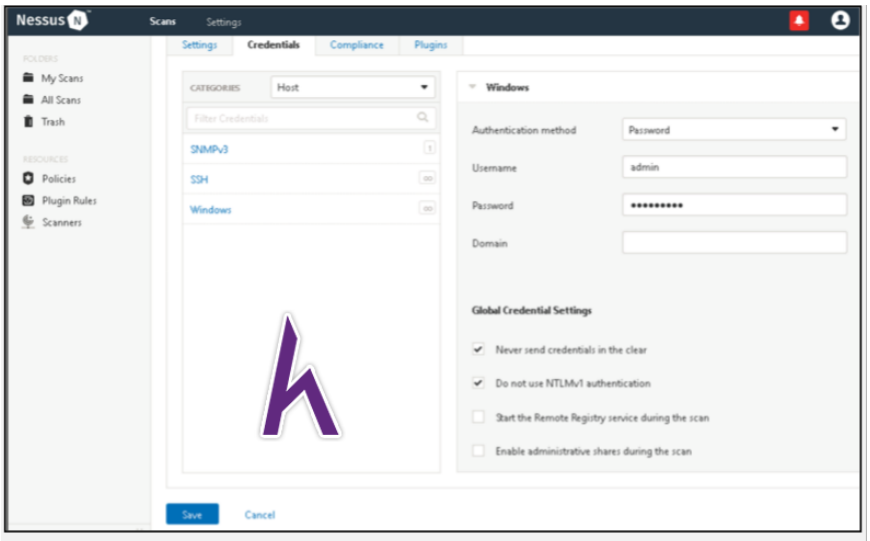

Figure 5-20 Configuring Policy

16. **Enable** hoặc **Disable** những plugins cần thiết.

17. Kiểm tra **Policy** xem đã configure thành công chưa.

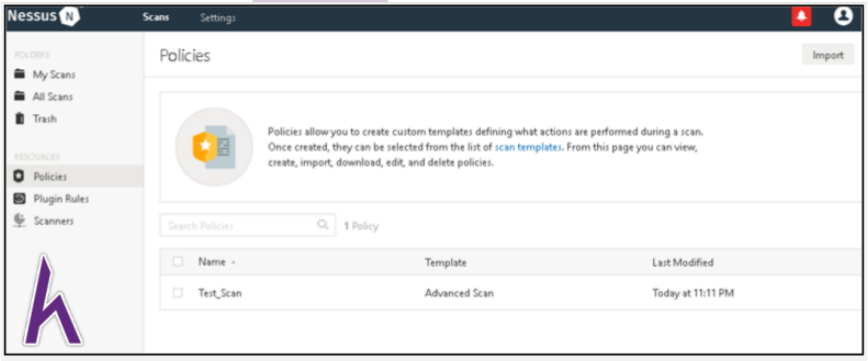

Figure 5-22 Verify Policy

18. Đến **Scan** > **Create New Scan**.

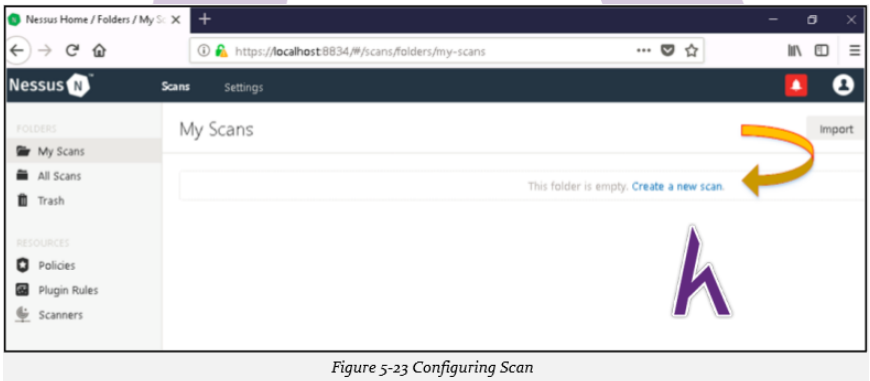

Figure 5-23 Configuring Scan

19. Đặt tên cho **New Scan**.

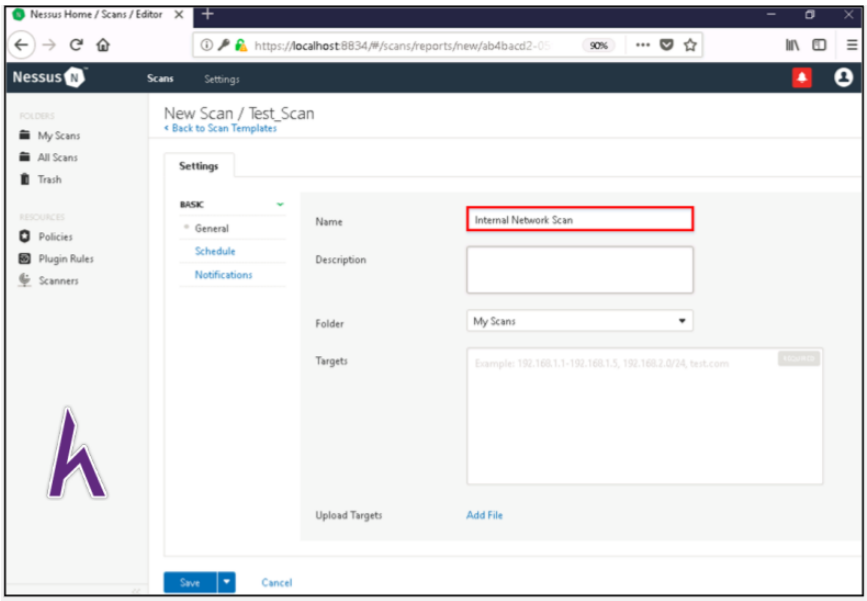

Figure 5-24 Configuring Scan

20. Nhập **Target Address**.

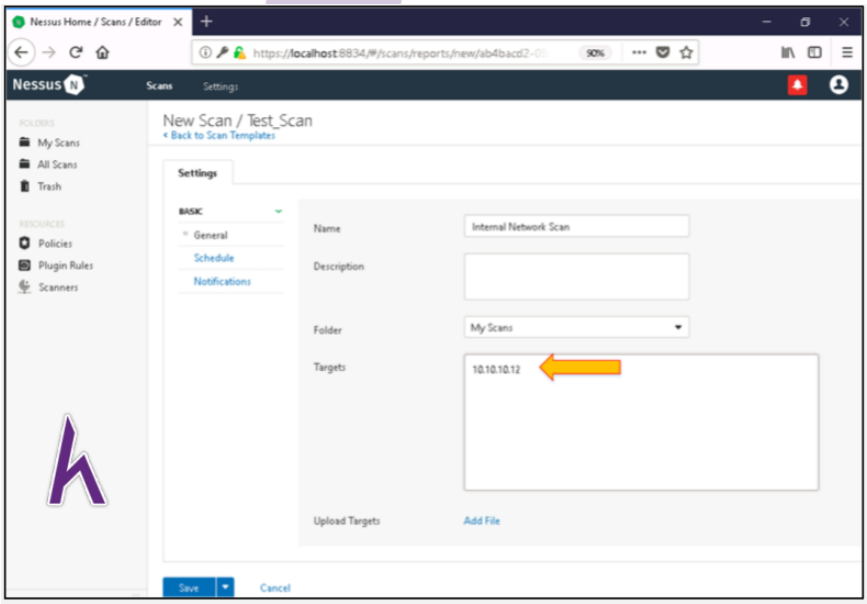

Figure 5-25 Configuring Scan

21. Đến **My Scan**, chọn **Scan** vừa tạo và chọn **Launch**.

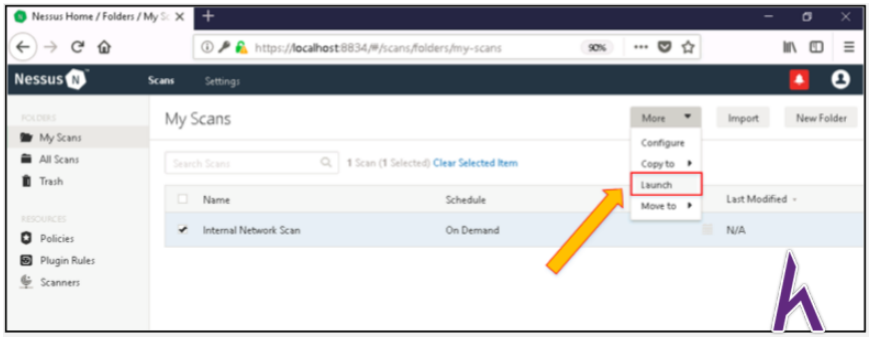

Figure 5-26 Launching Scan

22. Quan sát trạng thái để đảm bảo bắt đầu Scan thành công.

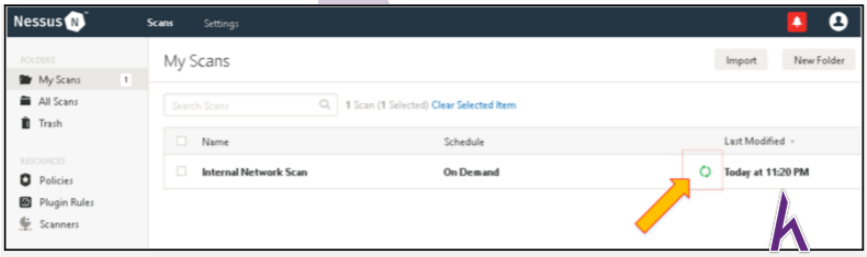

Figure 5-27 Scanning

23. Quan sát kết quả sau khi hoàn thành.

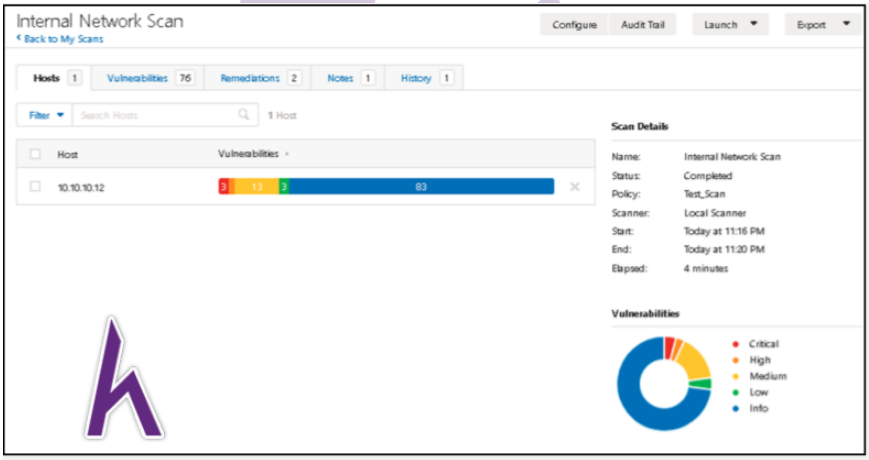

Figure 5-28 Scan results

24. Click vào **Vulnerabilities Tab** để quan sát các lỗ hổng được tìm thấy. Bạn cũng có thể vào các tab khác như **Remediation**, **Notes** và **History** để biết thêm thông tin về lịch sử, vấn đề và cách giảm thiểu rủi ro.

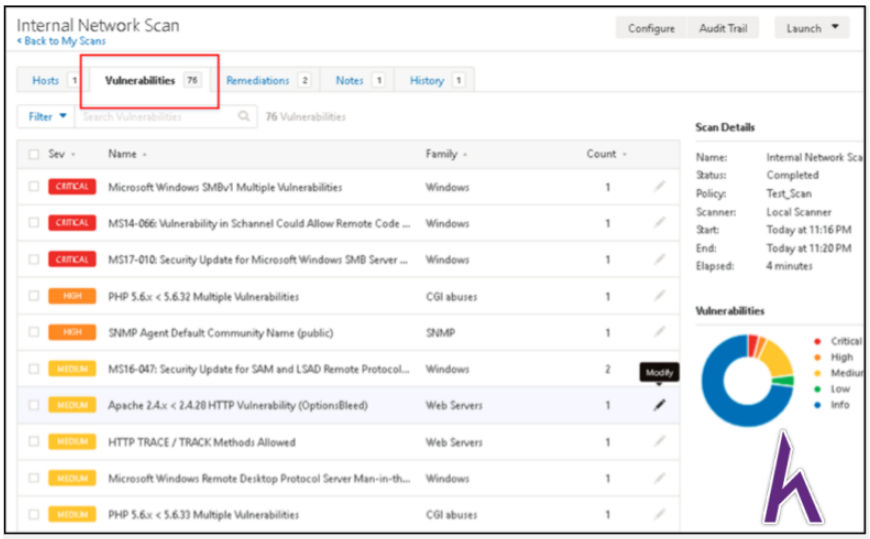

Figure 5-29 Scan results

25. Đến **Export tab** để xuất report và chọn format phù hợp.

26. Dưới đây là **preview** của report xuất ra trong định dạng PDF.