Mặc nhiên Nmap không có khả năng scan vulnerabilities như Nessus<Nmap chỉ là port scanner thôi> , tuy nhiên hiện nay đang có một số cố gắng sử dụng Nmap để quét các vul này <có thể xem thêm các link dưới đây:

<http://blog.rootshell.be/2010/06/03/vulnerability-scanner-within-nmap/>

<http://seclists.org/nmap-dev/2010/q2/538>

<http://seclists.org/nmap-dev/2010/q2/726>

>

Ý tưởng chính hết sức đơn giản như sau:

Sử dụng NSE script để chạy module quét version của các ứng dụng , khi đã có list các ứng dụng cũng như version này rồi thì map với cơ sở dữ liệu về các vul của OSVDB<Open Source Vulnerability Data Base> để có thể phát hiện ra các lỗi có thể có.

Tuy nhiên cách làm này hiện đang tồn tại vấn đề sau:

Cách đặt tên của Nmap và OSVDB khác nhau:

Ví dụ:

Apache :

Nmap: Apache httpd

OSVDB: Apache

OSVDB không hoàn toàn hỗ trợ việc link giữa tên phần mềm và lỗi

Ngoài ra cần cập nhật hệ thống cơ sở dữ liệu thường xuyên.