|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯ |
| HỌC PHẦN  **ĐÁNH GIÁ VÀ KIỂM ĐỊNH**  **AN TOÀN HỆ THỐNG THÔNG TIN** |
| BÀI THỰC HÀNH  **KIỂM THỬ AN TOÀN HỆ ĐIỀU HÀNH** |
| **Sinh viên thực hiện: HOÀNG NGUYÊN THÁI - AT14C** |
| **Hà Nội, 2021** |

MỤC LỤC

[*Phần 1. Thực hành kiểm thử an toàn hệ điều hành Windows XP* 3](#_Toc76974756)

[*Phần 2. Thực hành kiểm thử an toàn hệ điều hành Windows 7* 11](#_Toc76974757)

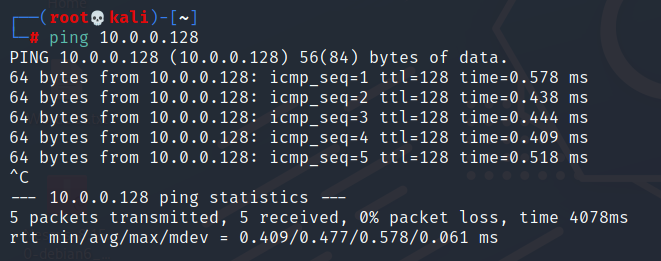
[*Phần 3. Thực hành kiểm thử an toàn hệ điều hành Windows Server* 15](#_Toc76974758)

# *Thực hành kiểm thử an toàn hệ điều hành Windows XP*

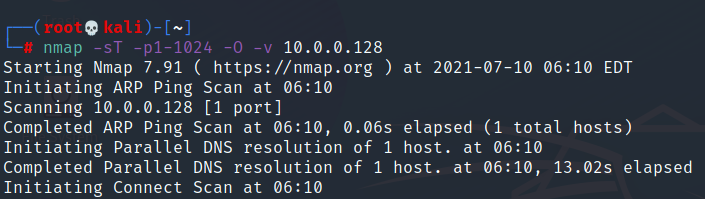
* Thông tin của máy nạn nhân (WinXP)

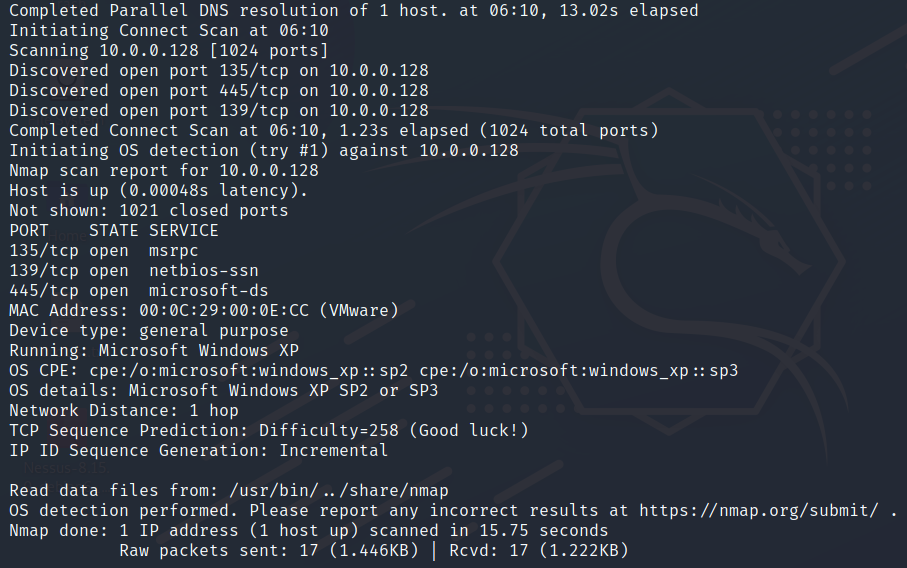


* Ping tới máy mục tiêu

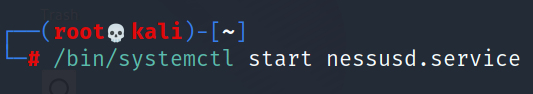


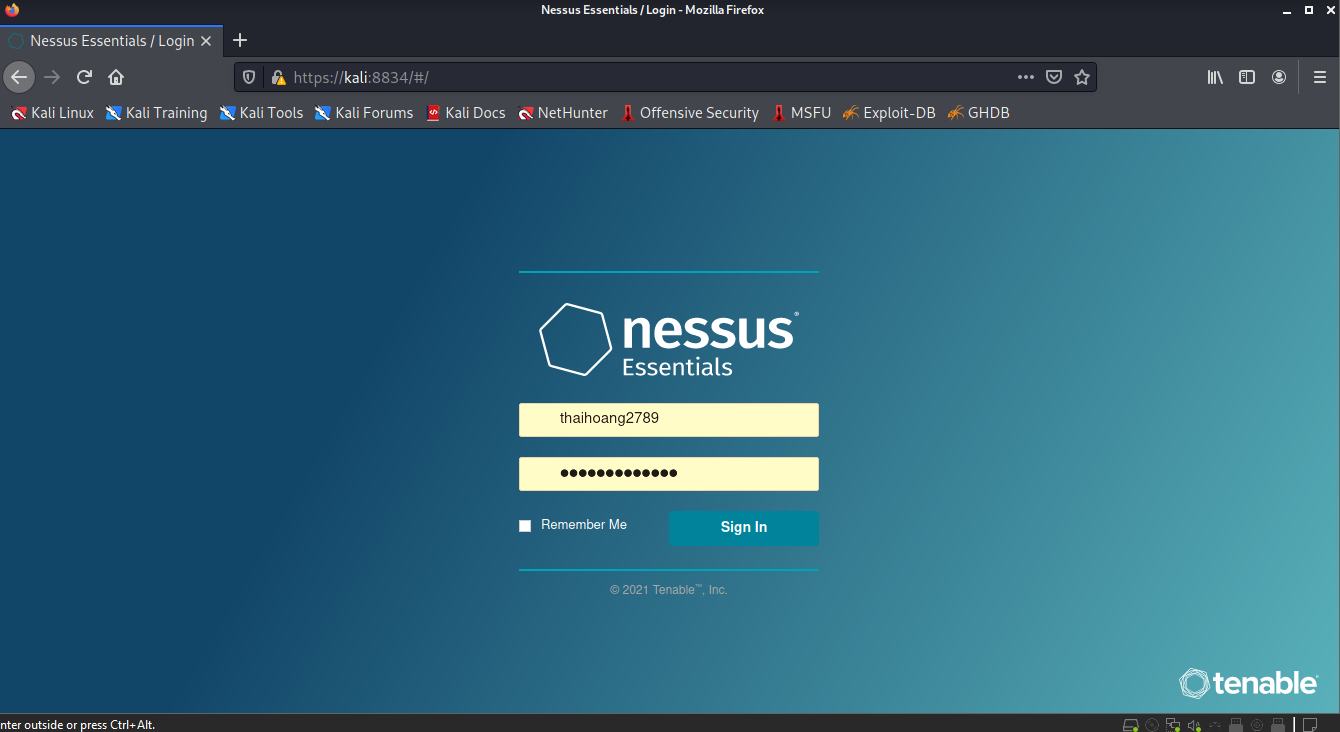
* Kiểm tra các cổng và dịch vụ bằng nmap

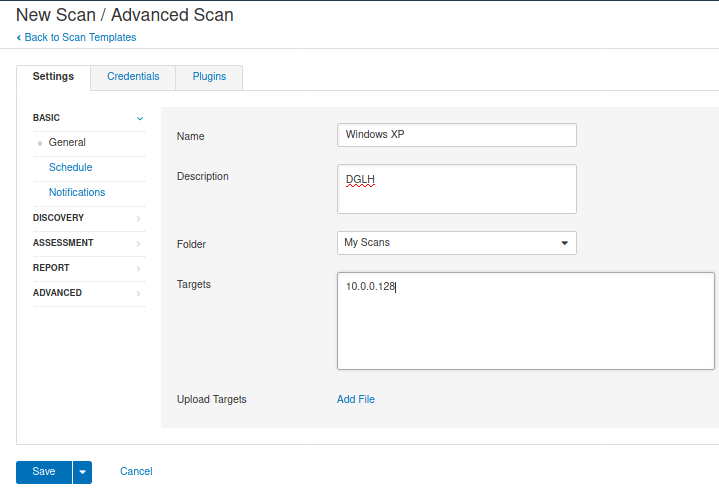


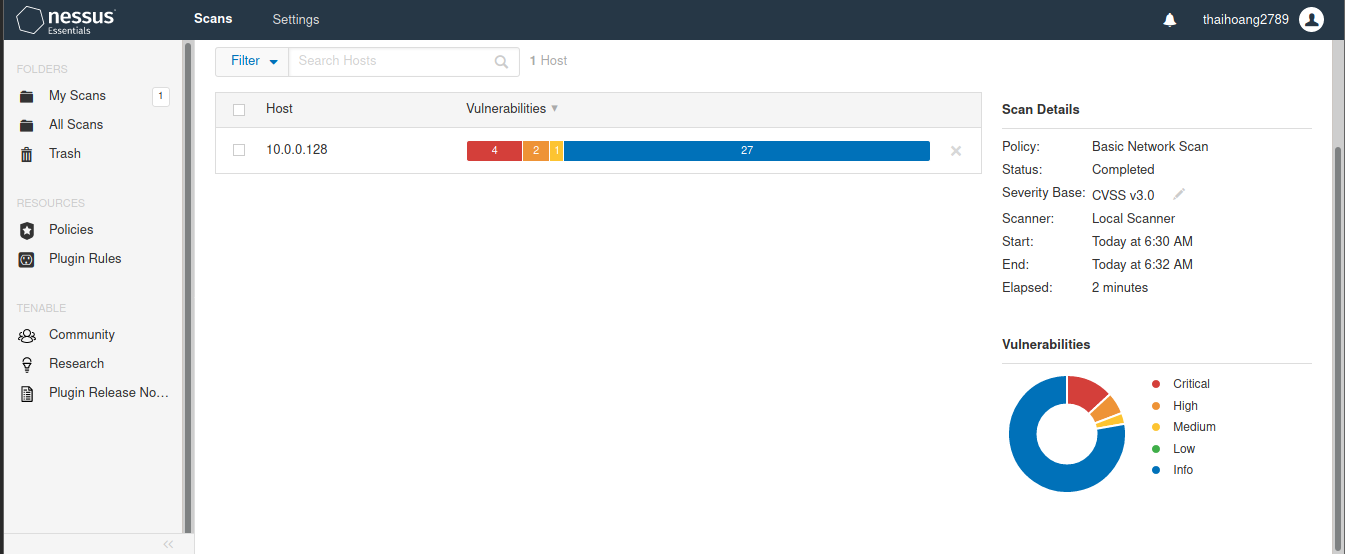


* Khởi chạy dịch vụ Nessus để quét lỗ hổng trên máy mục tiêu

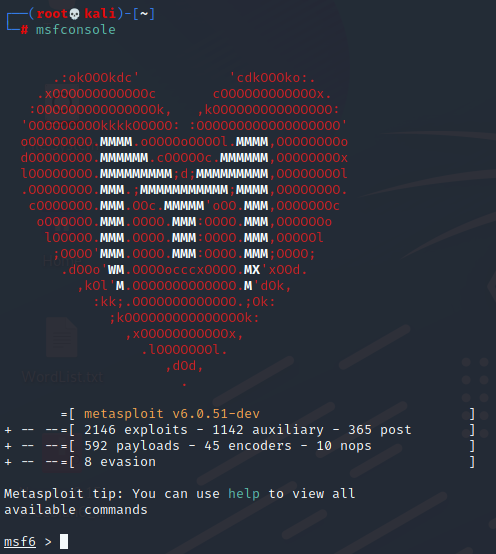


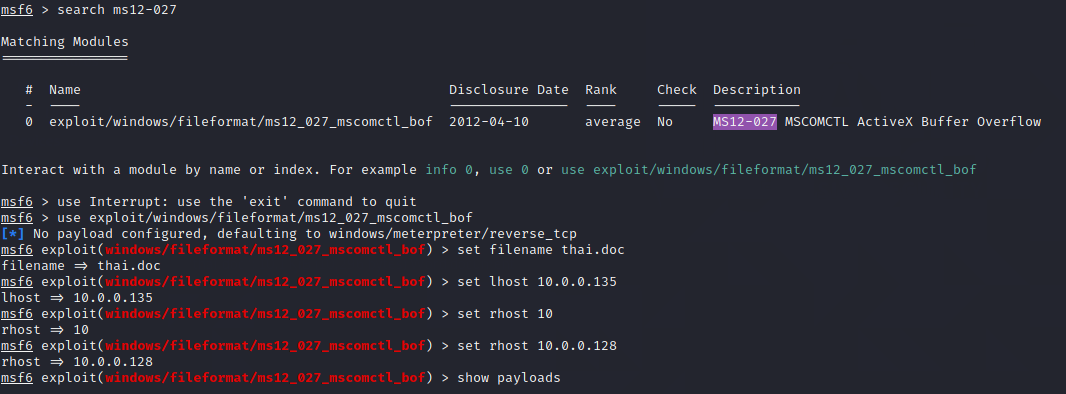


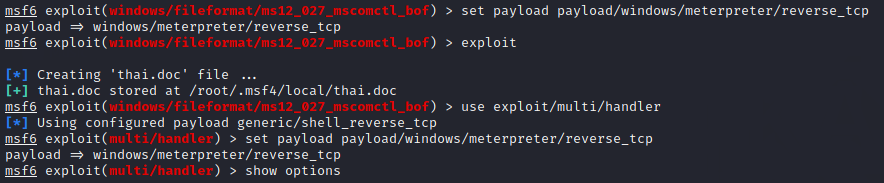


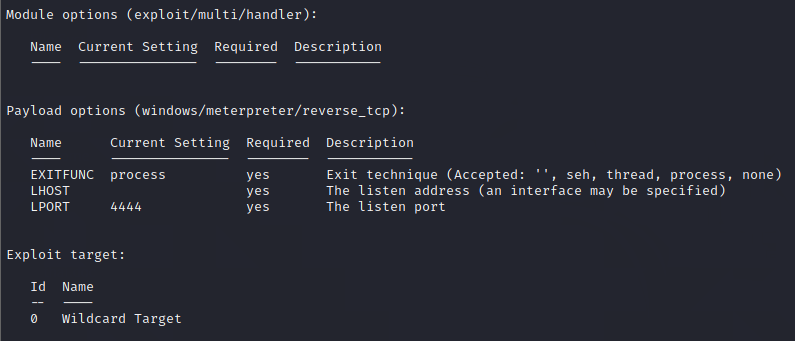


* Sử dụng Metasploit để khai thác lỗi ms12\_027

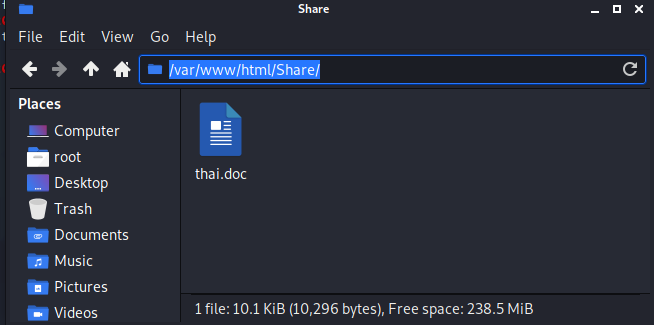


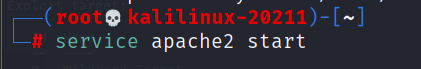


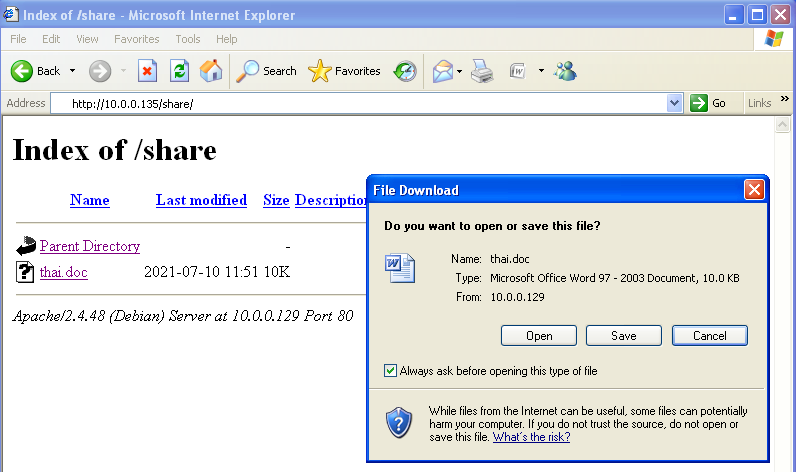




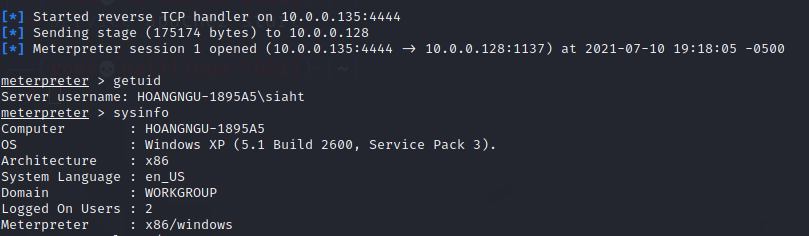


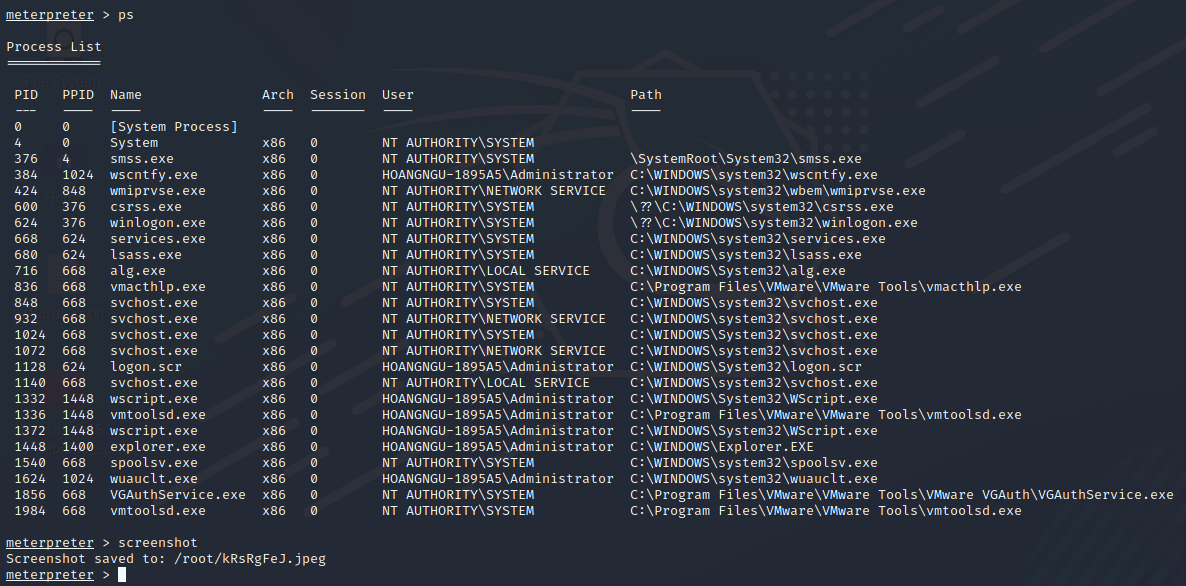


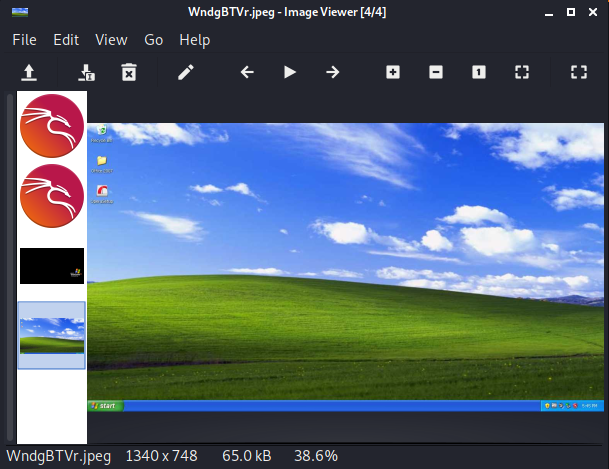


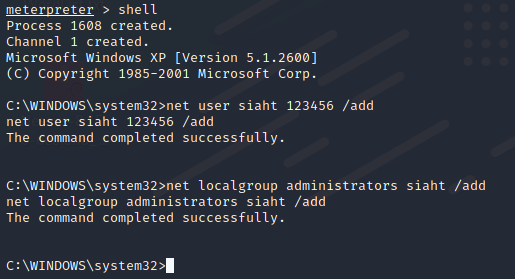


* Khi người dùng mở file lên chúng ta đã khai thác thành công

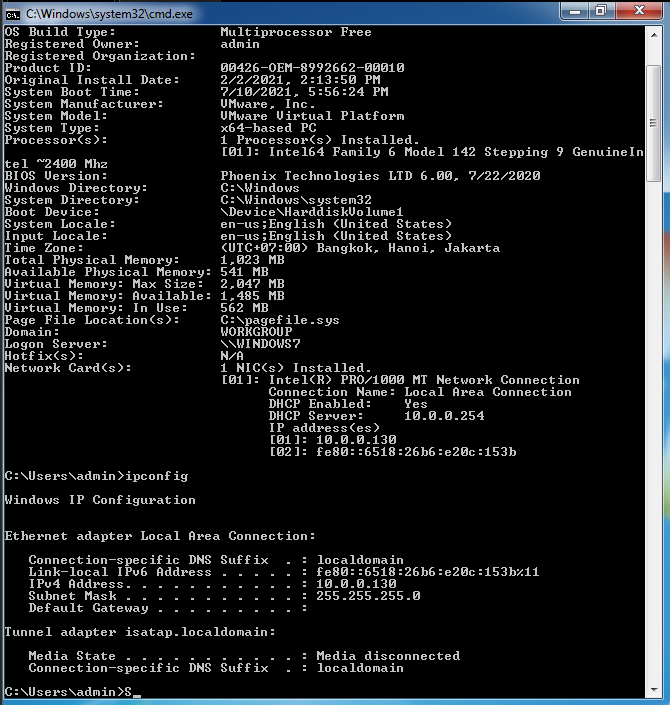


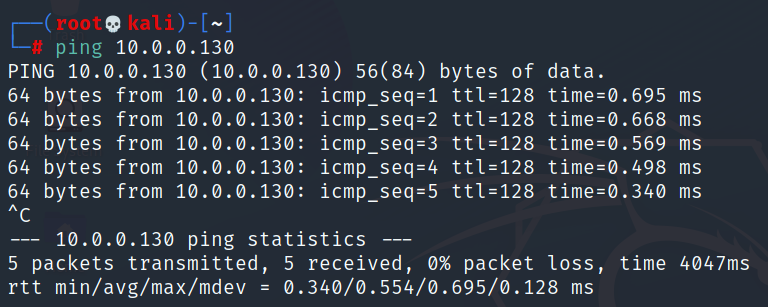


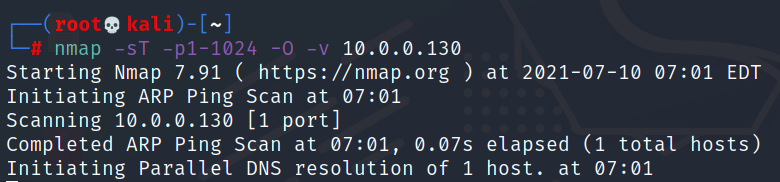


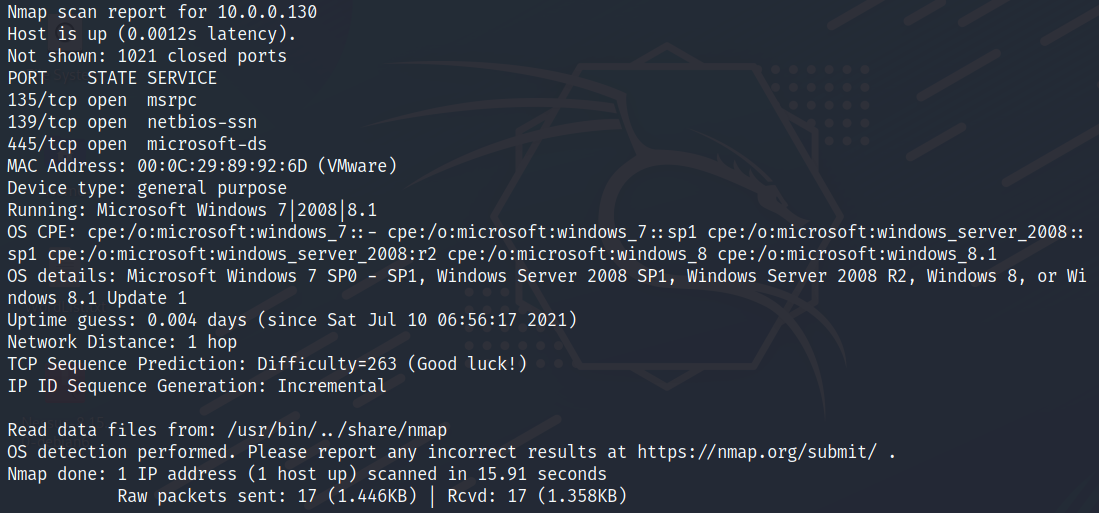


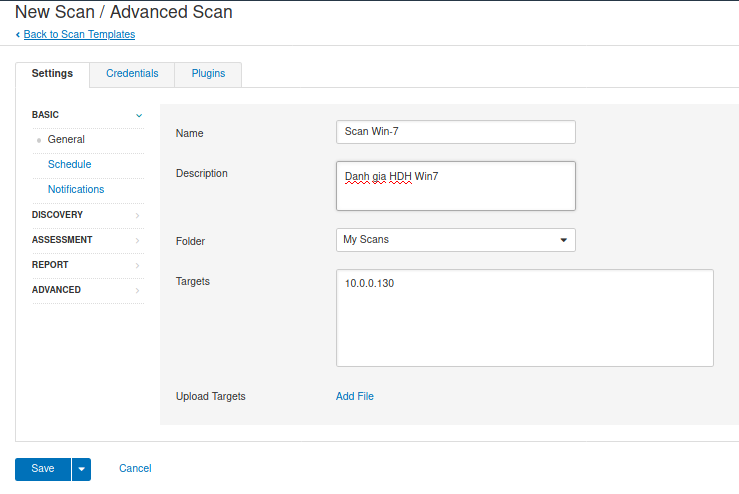
# *Thực hành kiểm thử an toàn hệ điều hành Windows 7*

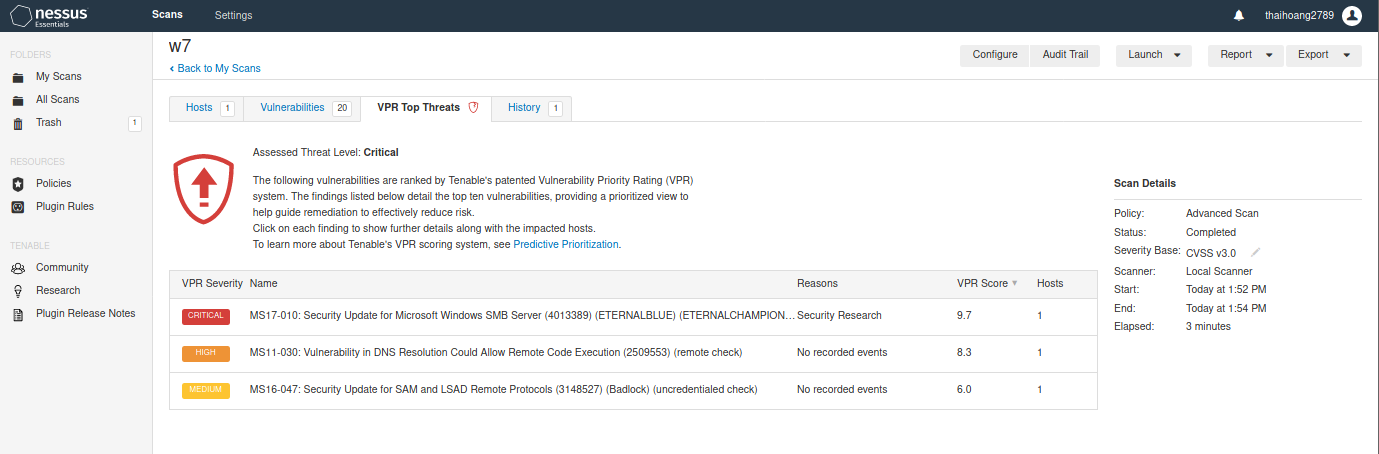


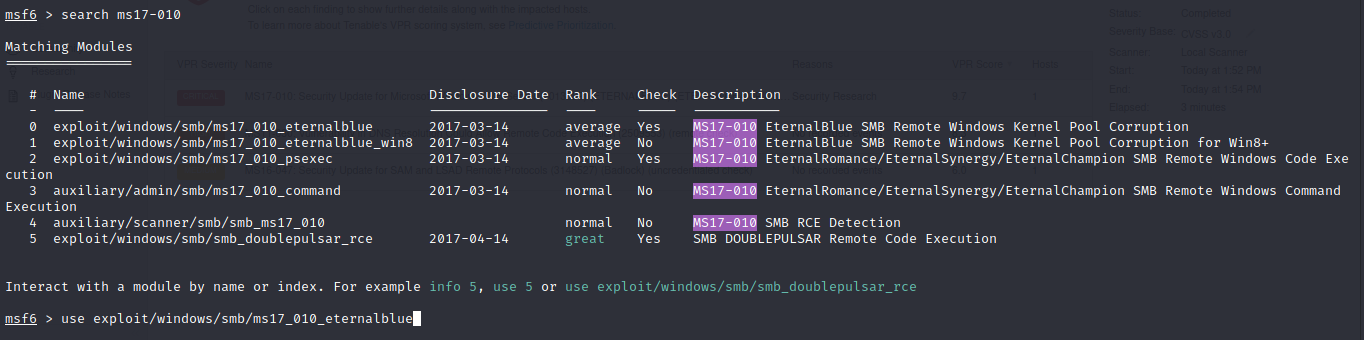


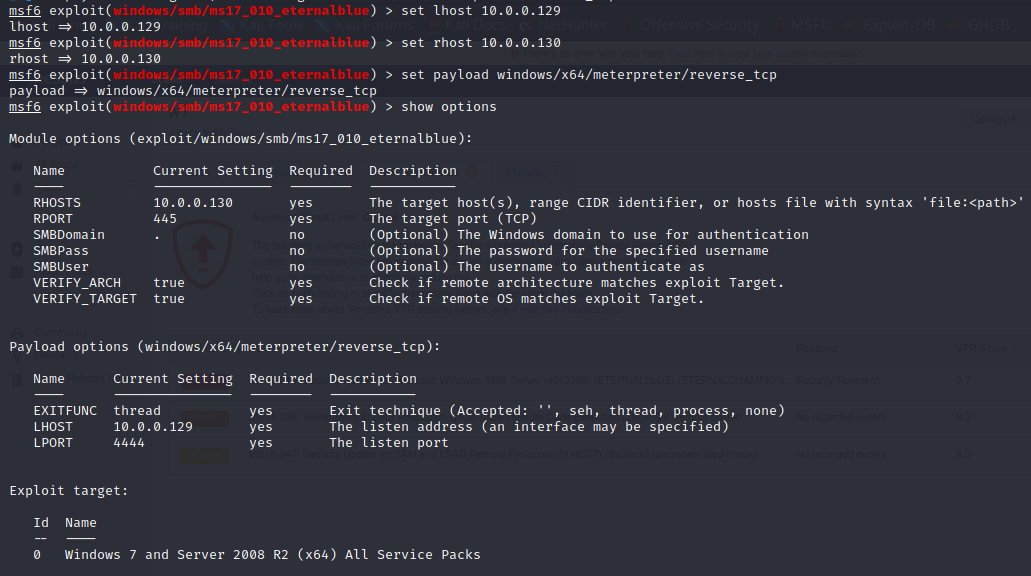


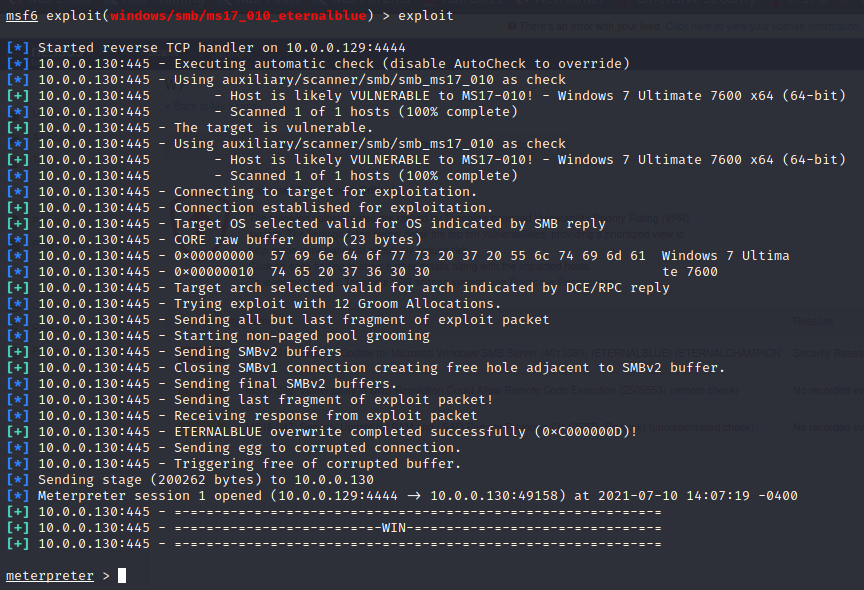


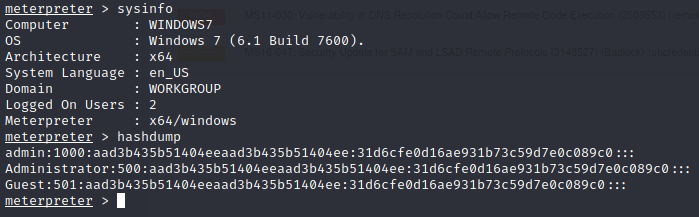












# *Thực hành kiểm thử an toàn hệ điều hành Windows Server*

