**Tìm kiếm và khai thác lỗ hổng**

**1. Mục đích**

- Hiểu được các mối đe dọa và lỗ hổng.

- Hiểu được cách thức hoạt động của một số công cụ rà quét và tìm kiếm đe dọa và

lỗ lổng như: nmap/zenmap, nessus, Metasploit framework.

- Biết cách sử dụng công cụ để tìm kiếm và khai thác các mối đe dọa, lỗ hổng bao

gồm: nmap/zenmap, nessus, Metasploit framework.

**2. Nội dung thực hành**

**2.1 Tìm hiểu lý thuyết**

**Tìm hiểu về nmap/zenmap, nessus, metasploit framework**

**a. Nmap/Zenmap:**

- Nmap (tên đầy đủ Network Mapper) là một công cụ bảo mật được phát triển bởi Floydor Vaskovitch. Nmap có mã nguồn mở, miễn phí, dùng để quét cổng và lỗ hổng bảo mật. Các chuyên gia quản trị mạng sử dụng Nmap để xác định xem thiết bị nào đang chạy trên hệ thống của họ, cũng như tìm kiếm ra các máy chủ có sẵn và các dịch vụ mà các máy chủ này cung cấp, đồng thời dò tìm các cổng mở và phát hiện các nguy cơ về bảo mật.

- Mặc dù Nmap đã không ngừng được phát triển, cải tiến qua nhiều năm và cực kỳ linh hoạt, nhưng nền tảng của nó vẫn là một công cụ quét cổng, thu thập thông tin bằng cách gửi các gói dữ liệu thô đến các cổng hệ thống. Sau đó nó lắng nghe và phân tích các phản hồi và xác định xem các cổng đó được mở, đóng hoặc lọc theo một cách nào đó, ví dụ như tường lửa. Các thuật ngữ khác được sử dụng để chỉ hoạt động quét cổng (port scanning) bao gồm dò tìm cổng (discovery) hoặc liệt kê cổng (enumeration).

- Nmap quét cổng:

* 80/443 mở có nghĩa là dịch vụ web đang hoạt động
* Cổng 25 mở có nghĩa là dịch vụ gửi thư/ nhận email SMTP đang hoạt đông
* Cổng 1433 mở có nghĩa là máy chủ Microsoft SQL Server đang hoạt động
* Cổng 53 mở có nghĩa là dịch vụ tên miền DNS đang hoạt động

**b. Nessus**

- Nessus-sản phẩm của công ty Tenable: là một công cụ dò quét lỗ hổng hệ thống, ứng dụng web và các thiết bị mạng rất mạnh. Nessus được sử dụng bởi rất nhiều chuyên gia đánh giá bảo mật. Với hệ thống các plug-ins, cơ sở dữ liệu lỗ hổng luôn được cập nhật, Nessus là sự lựa chọn hàng đầu cho việc dò quét lỗ hổng. Nessus bao gồm có 4 phiên bản: Nessus Home, Nessus Professional, Nessus Manager và Nessus Cloud. Trong đó, Nessus Home là phiên bản miễn phí và giới hạn một số tính năng về đánh giá bảo mật.

- Ban đầu Nessus là một dự án nguồn mở “Nessus Project” được đề xuất bởi Renaud Derasion vào năm 1998, mã nguồn của các thành phần được công bố công khai.

- Nessus cho phép quét các loại lỗ hổng:

* Lỗ hổng cho phép một hacker từ xa kiểm soát hoặc truy cập dữ liệu nhạy cảm trên hệ thống
* Cấu hình sai (ví dụ như chuyển tiếp thư mở, các bản vá lỗi bị thiếu,...).
* Tấn công từ chối dịch vụ bộ nhớ stack TCP/IP bằng gói tin độc hại
* Chuẩn bị cho việc kiểm tra bảo mật

**c. Metasploit Framework**

- Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service. Metasploit được xây dựng từ ngôn ngữ hướng đối tượng Perl, với những component được viết bằng C, assembler, và Python. Metasploit có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS. Có thể download chương trình tại metasploit.com.

- Metasploit có thể tự động update bắt đầu từ version 2.2 trở đi, sử dụng script msfupdate.bat trong thư mục cài đặt.

- Metasploit hỗ trợ nhiều giao diện với người dùng:

* Console interface: Dùng msfconsole.bat. Msfconsole interface sử dụng các dòng lệnh để cấu hình, kiểm tra nên nhanh hơn và mềm dẻo hơn
* Web interface: Dùng msfweb.bat, giao tiếp với người dùng thông qua giao diện Web
* Command line interface: Dùng msfcli.bat

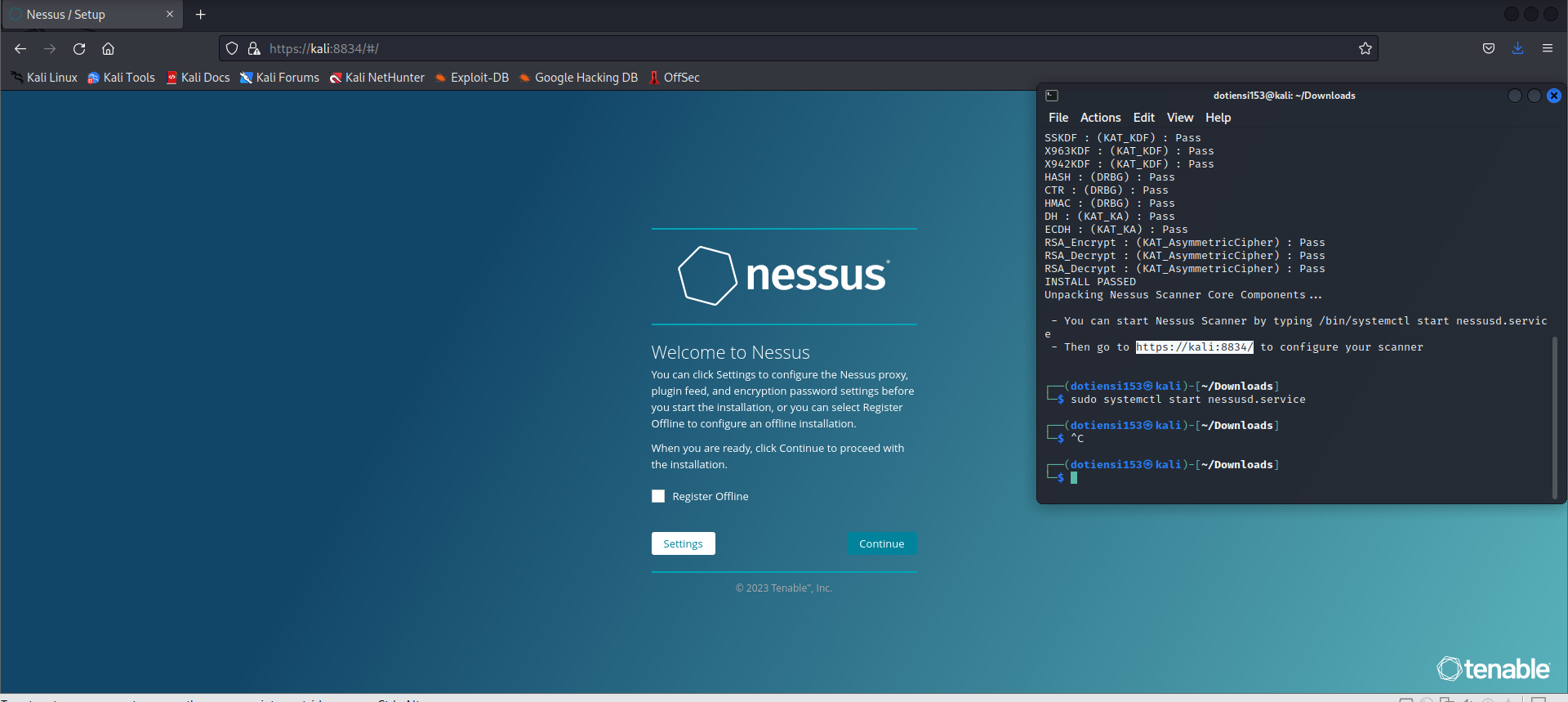
- Command line interface: Dùng msfcli.bat

* Lỗ hổng eternalblue: là một khai thác thông tin được phát triển bởi Cục An ninh Quốc gia Hoa Kỳ(NSA). Nó đã bị rò rỉ bởi những nhóm hacker The Shadow Brokers vào ngày 14 tháng 4 năm 2017, và đã sử dụng như là một phần của Vụ tấn công WannaCry trên toàn thế giới vào ngày 12 Tháng năm 2017.
* EternalBlue khai thác một lỗ hổng trong việc triển khai thực hiện giao thức SMB (Server Message Block) của Microsoft. Lỗ hổng này được biểu thị bằng mục CVE-2017-0144 trong mục Danh mục Khiếm ẩn Chung và Phơi nhiễm (CVE). Các lỗ hổng tồn tại tại bởi vì máy chủ SMBv1 1 trong các phiên bản khác nhau của Microsoft Windows chấp nhận các gói dữ liệu đặc biệt được tạo bởi những kẻ tấn công từ xa, cho phép họ thực thi mã tùy ý trên máy tính mục tiêu
* Bản cập nhật bảo mật Windows tiêu chuẩn vào ngày 14 Tháng 3 năm 2017 đã giải quyết vấn đề thông qua cập nhật bảo mật MS17-010 cho tất cả các phiên bản Windows hiện đang được hỗ trợ tại thời điểm đó là Windows Vista,Windows 7, 8.1, Windows 10, Windows Server 2008, Windows Server 2012, và Windows Server 2016.
* Nhiều người dùng Windows khi đó đã không cài đặt MS17-010, hai tháng sau ngày 12 tháng 5 năm 2017, cuộc tấn công WannaCry đã sử dụng lỗ hổng EternalBlue để lây lan chính nó.
* Vào ngày 13 tháng 5 năm 2017, một ngày sau cuộc tấn công, Microsoft đã thực hiện một bước rất khác thường trong việc cung cấp bản cập nhật bảo mật cho Windows XP, Windows 8, và Windows Server 2003 qua tải về từ Microsoft Bản danh Mục.Cài đặt nessus

Text

Description automatically generated

Cài đặt thành công



Máy kali

Text

Description automatically generated

Máy Windows 7

Text

Description automatically generated with medium confidence

Dùng nmap để quét các dịch vụ đang mở trên các cổng

Text

Description automatically generatedText

Description automatically generated

Sử dụng nessus để quét các lỗ hổng mạng

Graphical user interface, text, application

Description automatically generated Graphical user interface, text, application

Description automatically generated

A screenshot of a computer

Description automatically generated Text

Description automatically generated Text

Description automatically generated A screenshot of a computer

Description automatically generated Ta chọn lỗ hổng MS17-010 để khai thác:

Dùng search MS17-010 để xem các phương thức được hỗ trợ

Graphical user interface

Description automatically generated

Khai thác lỗ hổng thành công

Text

Description automatically generated