|  |
| --- |
| HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  **KHOA CÔNG NGHỆ THÔNG TIN 1** |
|  |
| **BÀI THỰC HÀNH 11**  **THỰC TẬP CƠ SỞ** |
| **Họ và tên : Đinh Quang Hiếu**  **Mã sinh viên: B19DCAT065**  **Giảng viên giảng dạy: Hoàng Xuân Dậu** |
| **HÀ NỘI, THÁNG 4/2022** |

**Bài 11: Tìm kiếm và khai thác lỗ hổng**

**I. Lý thuyết**

* Tìm hiểu về nmap , nessus , metasploit framework
  + Nmap:
    - 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.
    - Nmap có thể được sử dụng để giám sát các máy chủ đơn lẻ cũng như các cụm mạng lớn bao gồm hàng trăm nghìn thiết bị và nhiều mạng con hợp thành.
  + Nessus:
    - Nessus là một công cụ quét lỗ hổng bảo mật độc quyền được phát triển bởi Công ty An ninh mạng Tenable, được phát hành miễn phí cho việc sử dụng phi thương mại.
    - 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,…).
      * Mật khẩu mặc định, một vài mật khẩu thường được sử dụng, và mật khẩu trống trên các tài khoản hệ thống. Nessus cũng có thể dùng Hydra (một công cụ bên thứ ba) để thực hiện một cuộc tấn công từ điển.
      * Tấn công từ chối dịch vụ bộ nhớ stack TCP/IP bằng gói tin độc hại
      * Chuẩn bị cho việc kiểm tra bảo mật (PSI DSS).
    - Trong hoạt động thông thường, Nessus bắt đầu bằng cách quét các cổng mạng qua một trong bốn bộ quét cổng mạng tích hợp sẵn (hay nó có thể sử dụng phần mềm quét AmapM hay Nmap) để xác định cổng đang mở trên mục tiêu và sau đó cố gắng thực hiện nhiều cách tấn công trên các cổng mở. Các bài kiểm tra lỗ hổng, có sẵn bằng việc đăng ký, được viết bằng NASL (ngôn ngữ tấn công dạng kịch bản Nessus – Nessus Attack Scripting Language), một ngôn ngữ kịch bản tối ưu cho tương tác mạng.
  + 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.
    - 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
    - Environment:
      * Global Environment: Được thực thi thông qua 2 câu lệnh setg và unsetg, những options được gán ở đây sẽ mang tính toàn cục, được đưa vào tất cả các module exploits.
      * Temporary Environment: Được thực thi thông qua 2 câu lệnh set và unset, environment này chỉ được đưa vào module exploit đang load hiện tại, không ảnh hưởng đến các module exploit khác.
    - Chức năng :
      * Quét cổng để xác định các dịch vụ đang hoạt động trên server.
      * Xác định các lỗ hổng dựa trên phiên bản của hệ điều hành và phiên bản các phần mềm cài đặt trên hệ điều hành đó.
      * Thử nghiệm khai thác các lỗ hổng đã được xác định.
* Một số lỗ hổng, cổng dịch vụ quét được quét được:
  + Port 139: Cổng 139 được sử dụng cho Chia sẻ tập tin và máy in
  + Port 445 : được dùng cho dịch vụ Server Message Block(SMB)
  + Lỗ hổng MS17 -010: là một trong những lỗ hổng bảo mật nghiêm trọng có thể gây thiệt hại lớn cho các doanh nghiệp tại Việt Nam. Tuy lỗ hổng MS17 -010 đã có bản vá lỗi nhưng trong quá trình đánh giá an ninh mạng cho các doanh nghiệp, SecurityBox nhận thấy một số đơn vị vẫn chưa cập nhật phiên bản phòng chống lỗ hổng này
  + Lỗ hổng MS16-047 : lỗ hổng bảo mật tồn tại trong quản lý tài khoản bảo mật (SAM) quyền bảo mật cục bộ (miền chính sách) (LSAD) từ xa giao thức khi họ chấp nhận mức xác thực không bảo vệ đầy đủ các giao thức. Lỗ hổng là bằng cách SAM và thiết lập giao thức từ xa LSAD kênh gọi thủ tục từ xa (RPC). Kẻ tấn công đã thành công khai thác lỗ hổng này có thể truy cập cơ sở dữ liệu SAM.
* Mô tả ngắn gọn về giao thức SMB :
  + SMB được viết tắt của từ Server Message Block, là một giao thức trong hệ điều hành Windows và DOS. SMB cung cấp cơ chế để các máy khách (client) có thể truy cập vào hệ thống file máy chủ (server), cũng như những thiết bị input/output (ví dụ như máy in).
  + Giao thức SMB đã được ra đời và đưa vào sử dụng từ giữa những năm 80 của thế kỷ 20 và trải qua nhiều phiên bản. Cụ thể, vào năm 1984 IBM đã ra SMB trong một bản công bố tài liệu về kỹ thuật của mình. Mục đích thiết kế ban đầu của SMB là một giao thức mạng để đặt tên và kiểm duyệt. Những phiên bản đầu tiên của SMB, hệ thống chia sẻ dữ liệu với các máy khách có quyền ngang nhau, tuy nhiên điều này chưa thực sự đảm bảo an toàn thông tin.
  + SMB là giao thức hoạt động theo cơ chế máy khách - máy chủ (request - response). Hiểu đơn giản là các máy khách sẽ gửi những yêu cầu đến máy chủ SMB sau đó máy chủ sẽ gửi phản hồi lại đến từng yêu cầu.
  + SMB còn có những chức năng quan trọng như:
    - Hỗ trợ tìm kiếm máy chủ sử dụng giao thức SMB khác.
    - Hỗ trợ in qua mạng.
    - Cho phép xác thực các file và thư mục được chia sẻ.
    - Thông báo những thay đổi của file và thư mục.
    - Xử lý những thuộc tính mở rộng của file.
    - Hỗ trợ dàn xếp, đàm phán để tương thích giữa các hình thái của SMB.
    - Cho phép khóa file đang truy cập tùy theo yêu cầu.

**II.Thực hành**

Chuẩn bị môi trường  
Máy ảo kali cài đặt công cụ tấn công

Graphical user interface, text, chat or text message

Description automatically generated

Text

Description automatically generated

* Các lỗ hổng các cổng dịch vụ quét bằng nmap

Text

Description automatically generated

Text

Description automatically generated

* Cài đặt nessus

Text

Description automatically generated

A computer screen with a blue background

Description automatically generated with low confidence

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Sử dụng metasploit framework tấn công

Tìm kiếm các cú pháp liên quan đến ms17\_010

Text

Description automatically generated

* Kiểm tra xem máy win7 có lỗi hay không

Text

Description automatically generated

* Chụp ảnh màn hình

Graphical user interface

Description automatically generated with medium confidence



**A screenshot of a computer

Description automatically generated**

* Xem thông tin

**Text

Description automatically generated**

* Tạo folder

**Text

Description automatically generated**

**Graphical user interface, text, application, email

Description automatically generated**