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

**Bài thực hành 3**

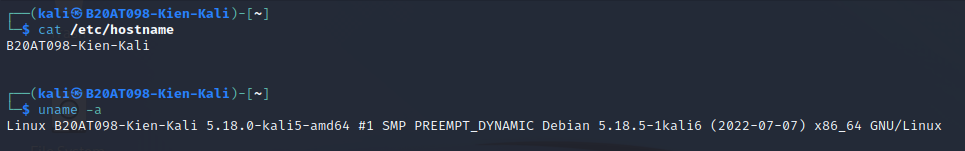
**Họ và tên: Hoàng Trung Kiên**

**Mã sinh viên: B20DCAT098**

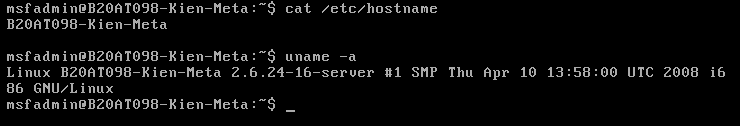
**1.Cài đặt các công cụ, nền tảng**

-Đổi tên hostname:

+Máy attacker:

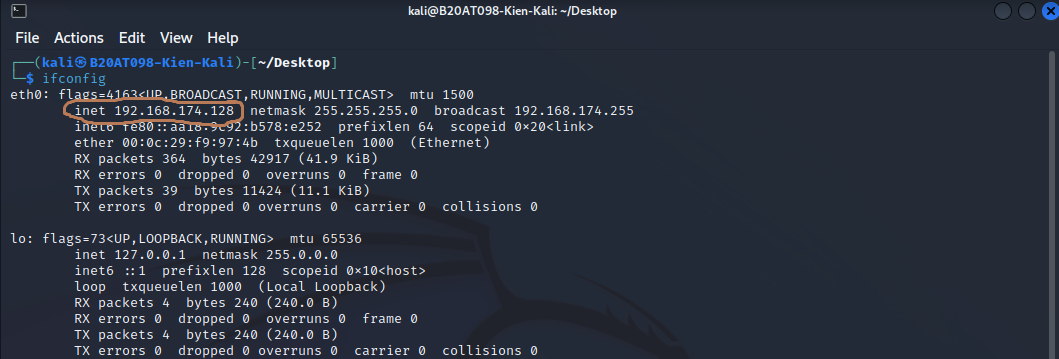


+Máy victim:



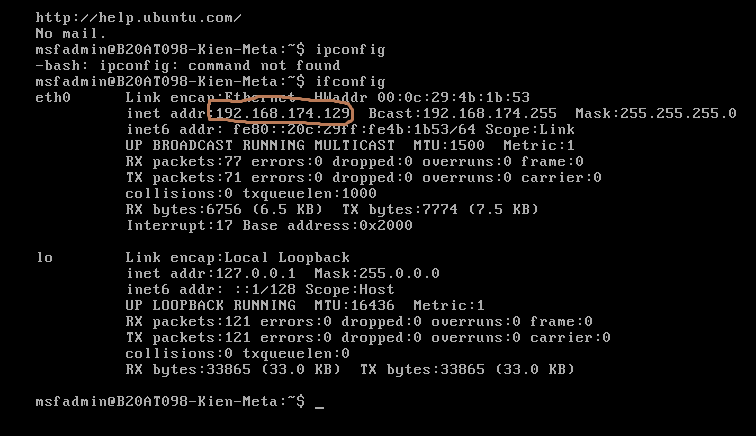
-Địa chỉ IP máy Kali:

+Địa chỉ ip máy attacker: 192.168.174.128



-Địa chỉ IP máy Metasploitable2:

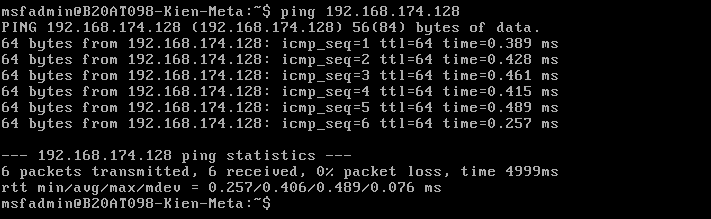
+Địa chỉ ip máy Victim: 192.168.174.129



\*Các máy ping nhau.

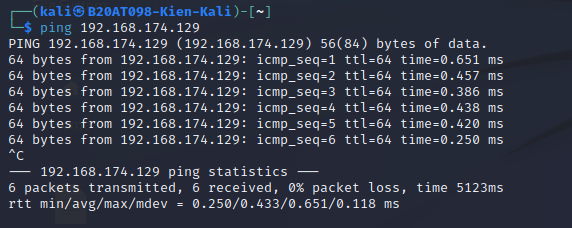
-Máy victim ping đến máy attacker

+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

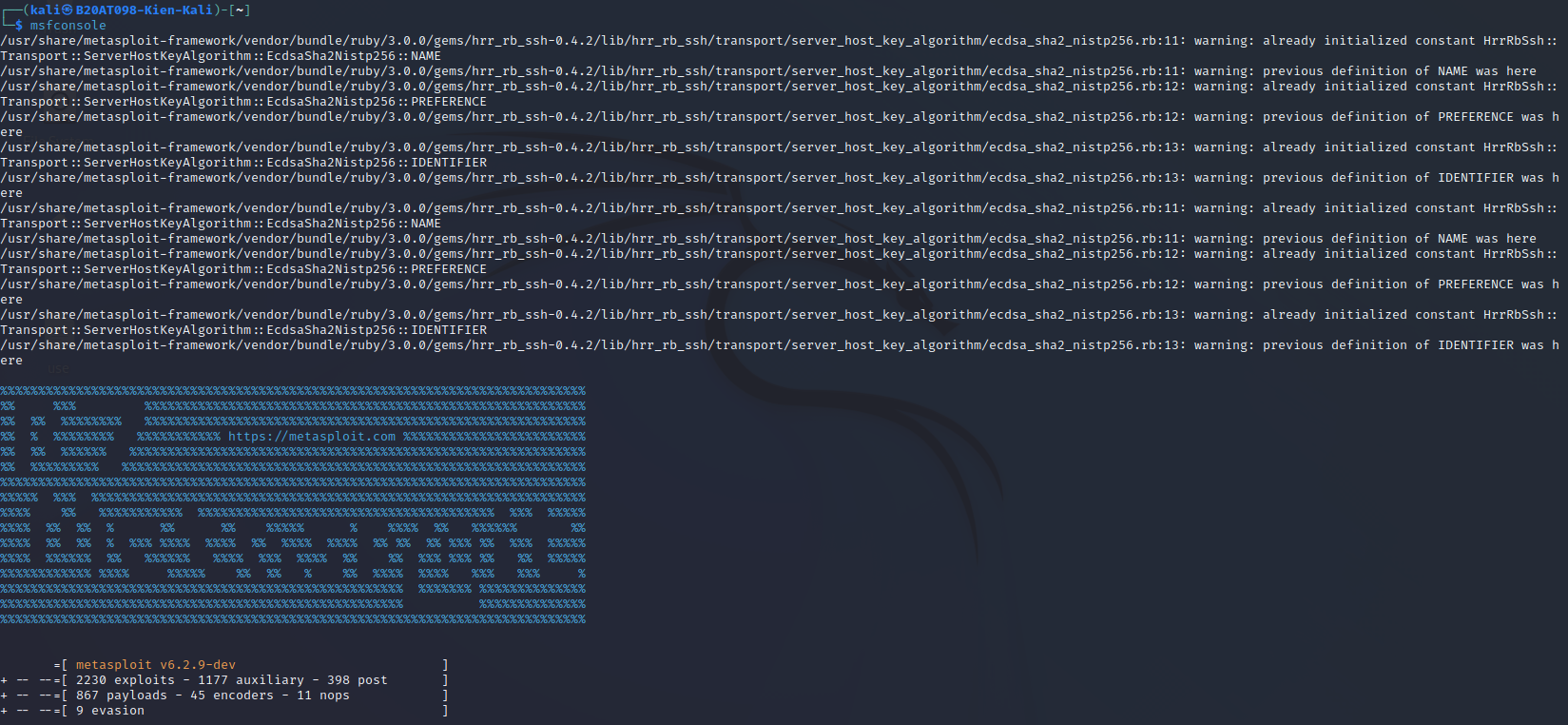


-Máy attacker ping đến máy victim:

+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



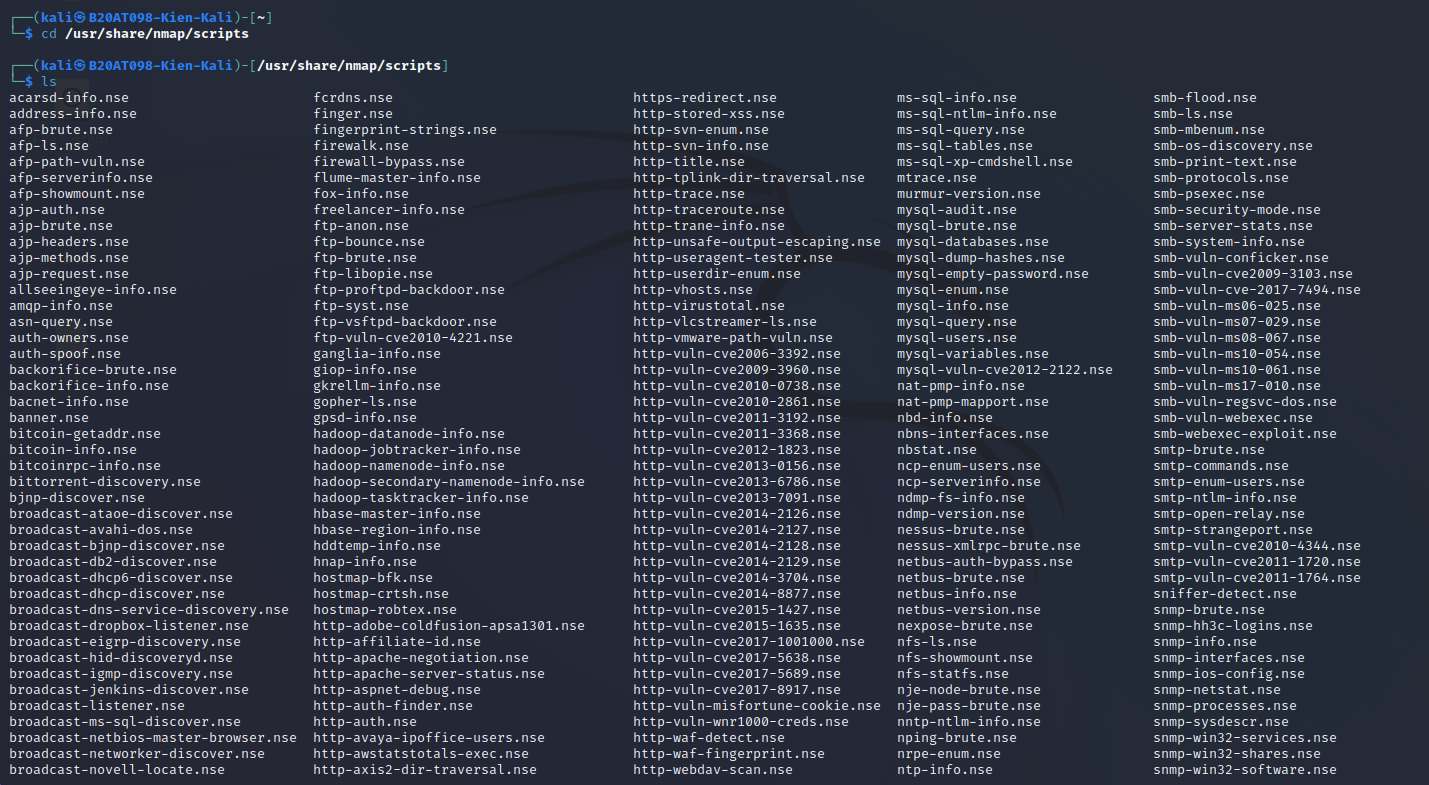
+Chạy công cụ msfconsole:

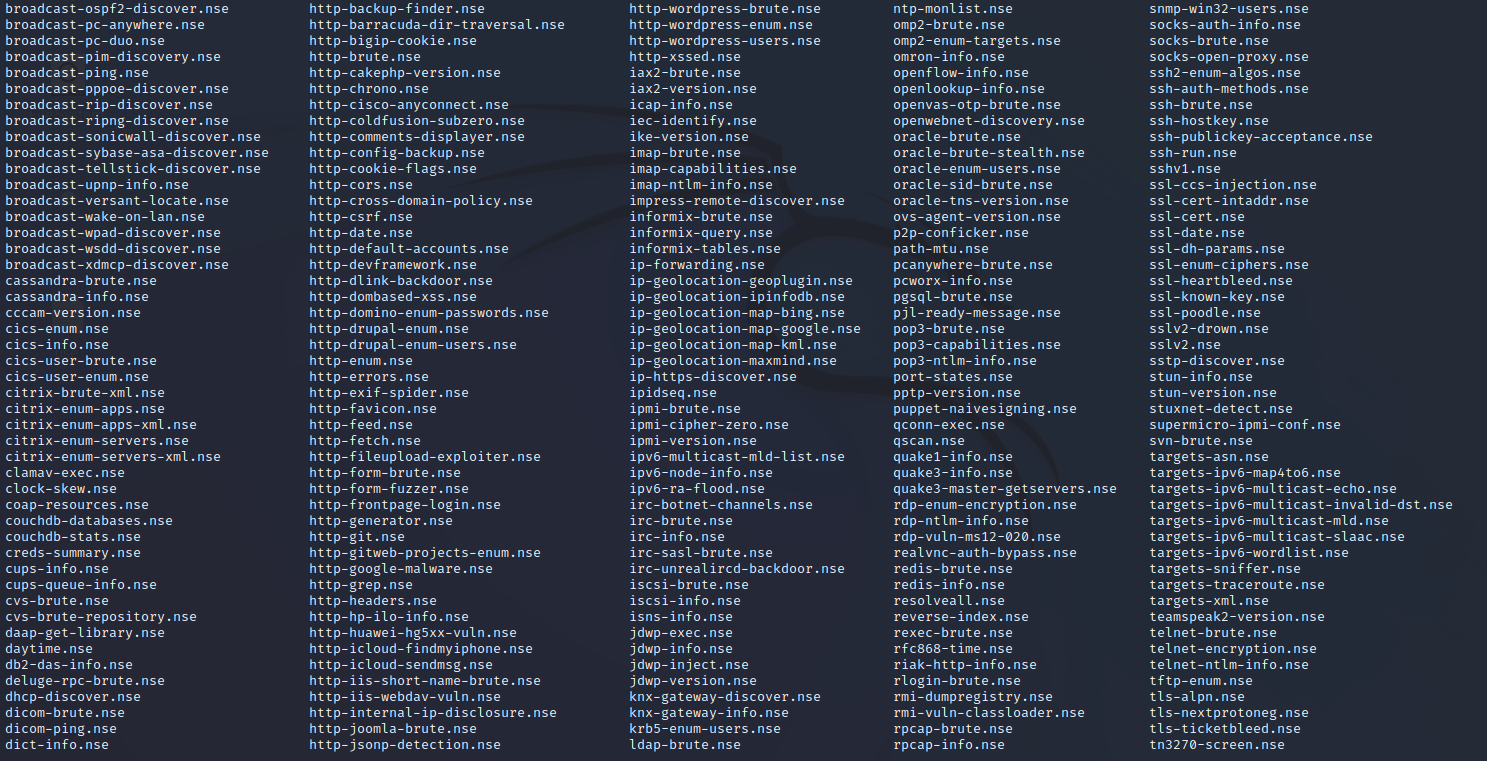


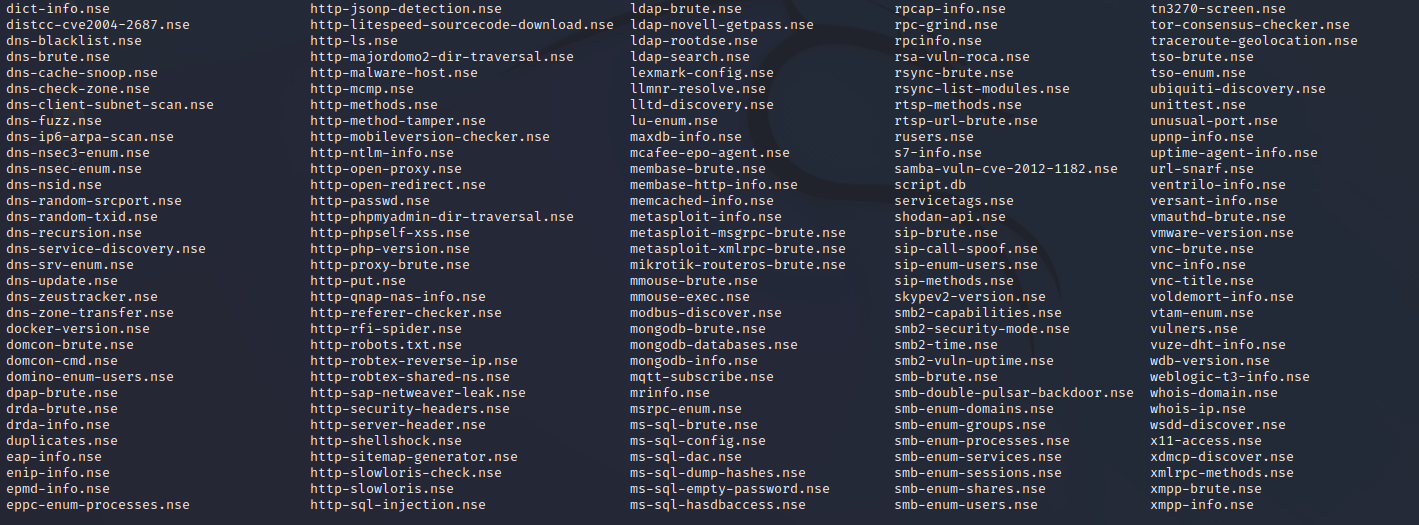
**2. Kiểm tra và cài đặt các NSE scripts cho nmap.**

-Kiểm tra các NSE scripts có sẵn cho nmap:

-> cd /usr/share/nmap/scripts



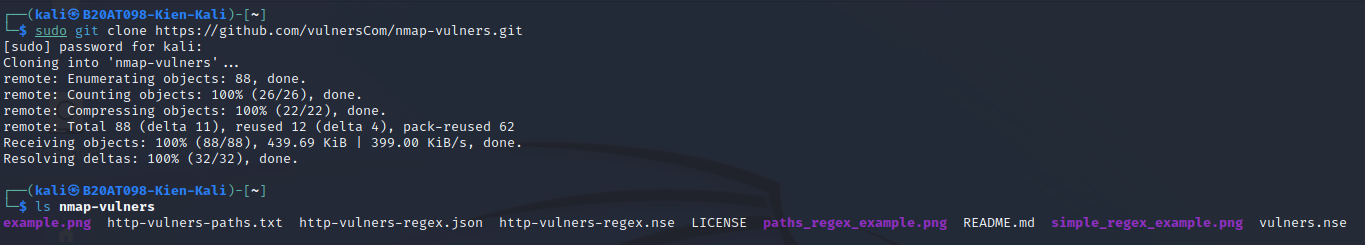




-Cài đặt CSDL nmap-vulners:

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

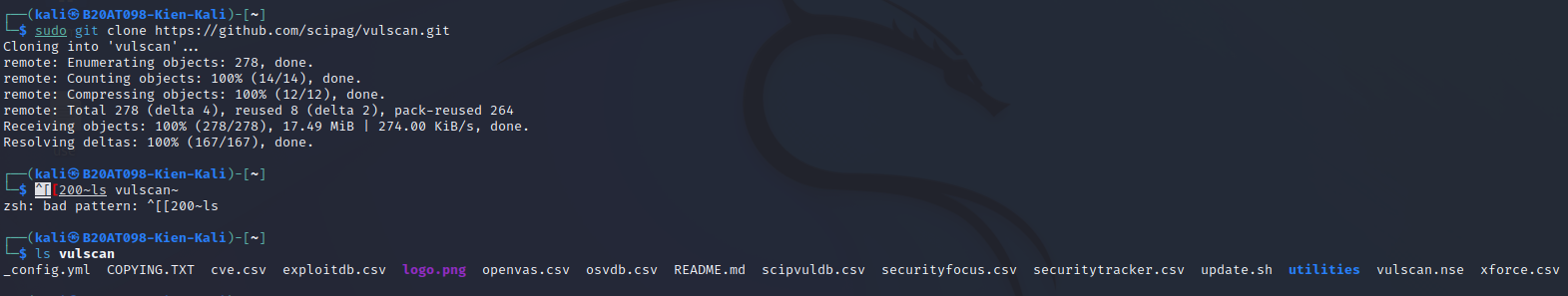
-> ls nmap-vulners



-Cài đặt CSDL:

-> vulscan: sudo git clone <https://github.com/scipag/vulscan.git>

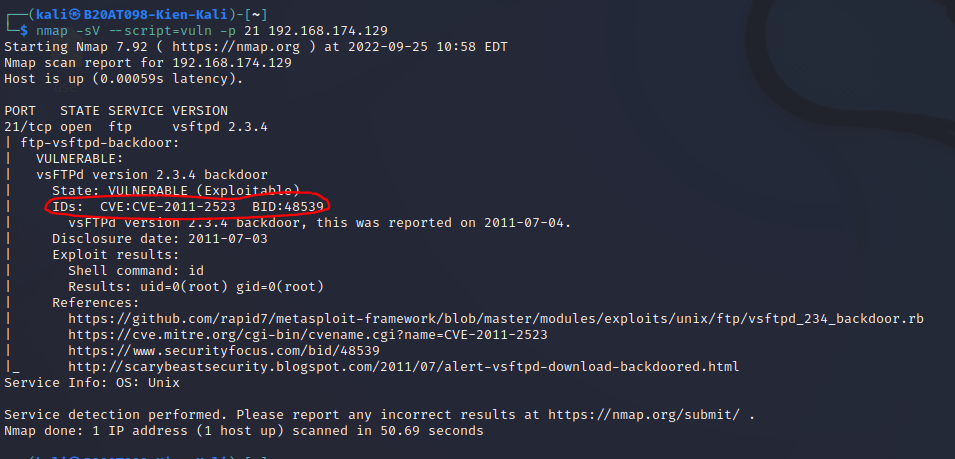
-> ls vulscan



**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.**

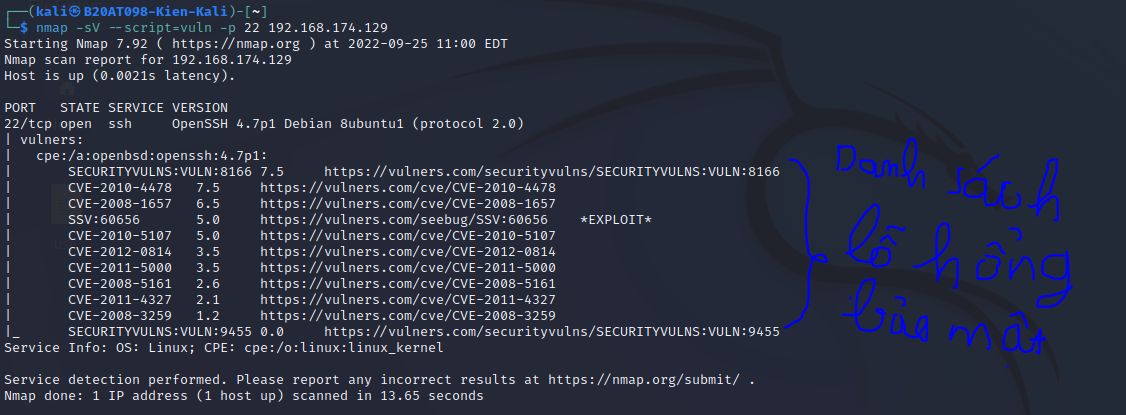
-Quét lỗ hổng bảo mật trên cổng 21 phía hệ thống victim:

-> nmap -sV --script=vuln -p 21 192.168.174.129



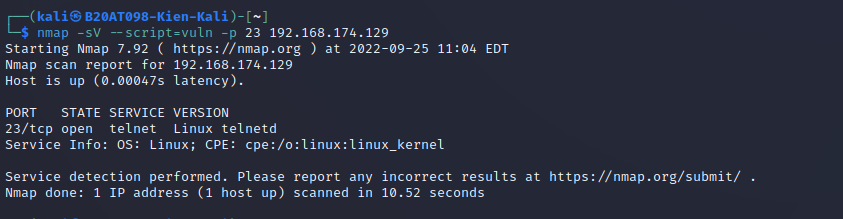
-Quét lỗ hổng bảo mật trên cổng 22 phía hệ thống victim:

-> nmap -sV --script=vuln -p 22 192.168.174.129



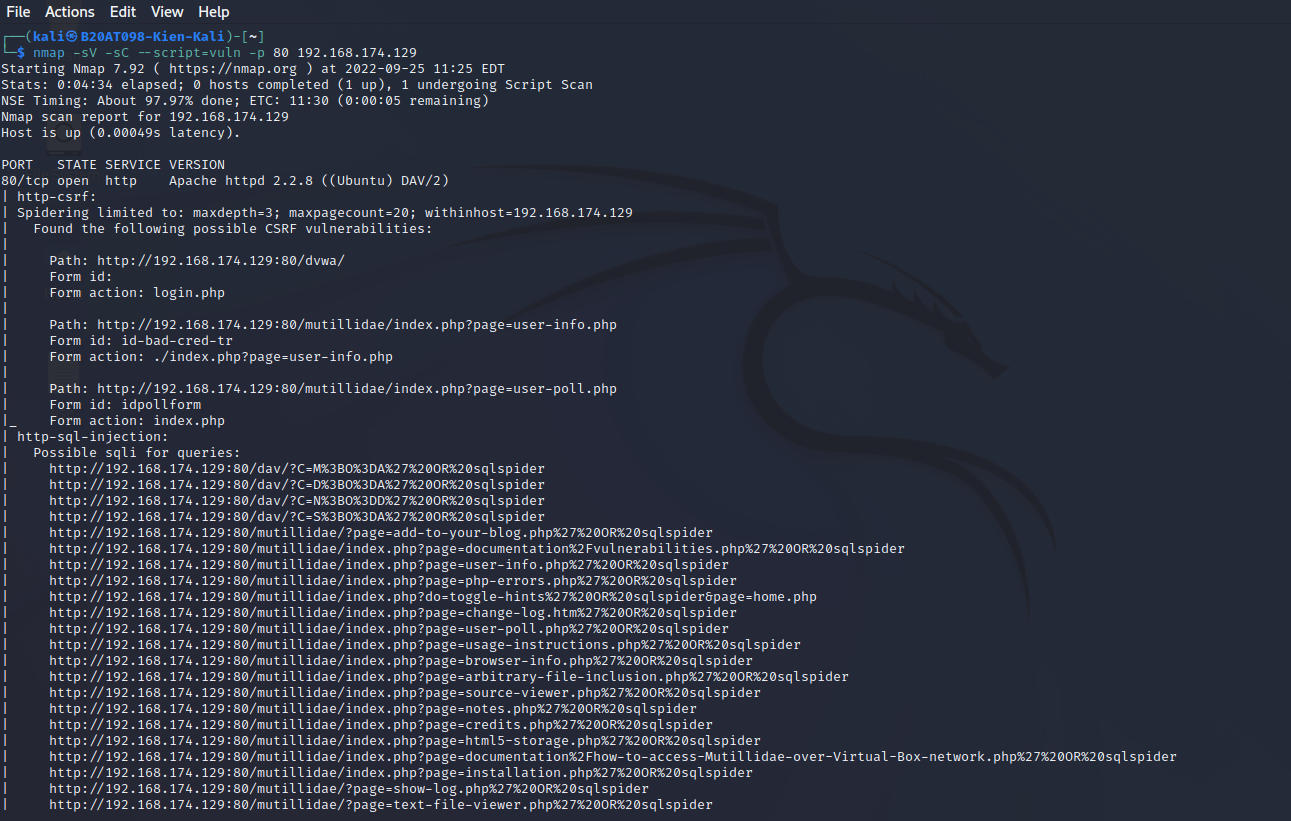
-Quét lỗ hổng bảo mật trên cổng 23 phía hệ thống victim:

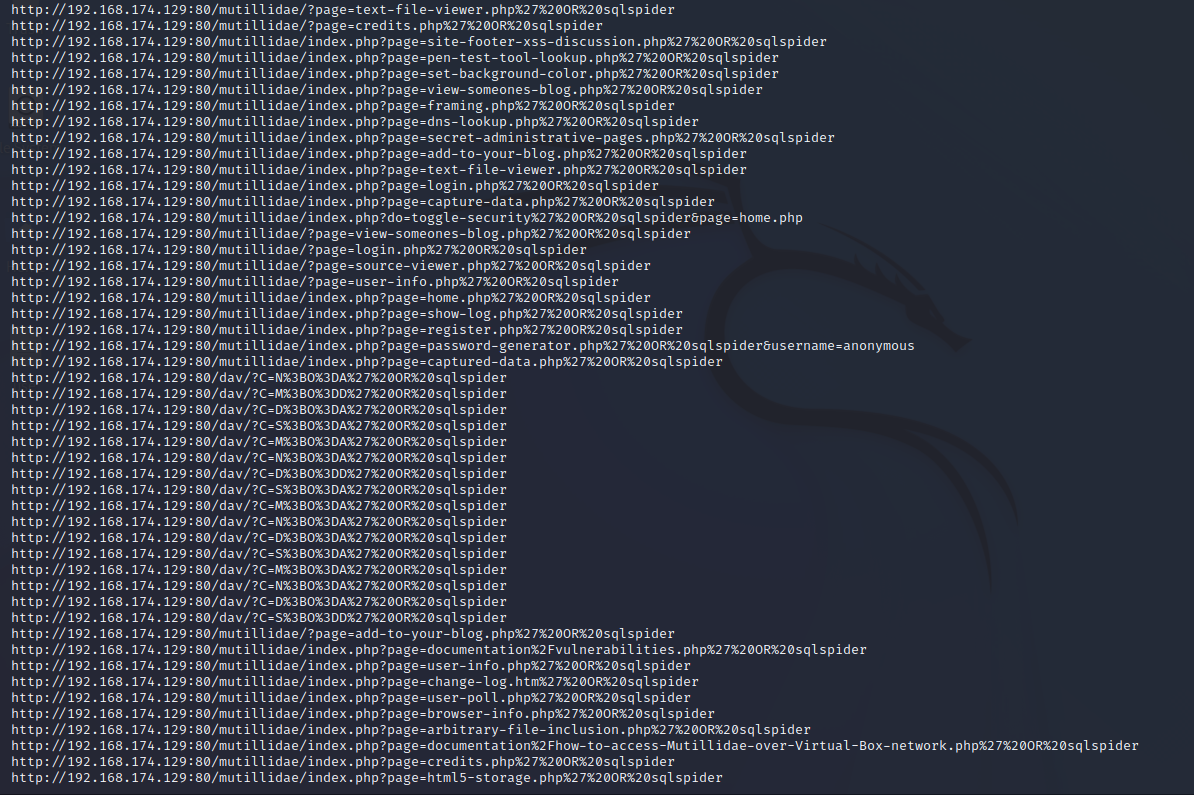
-> nmap -sV --script=vuln -p 23 192.168.174.129

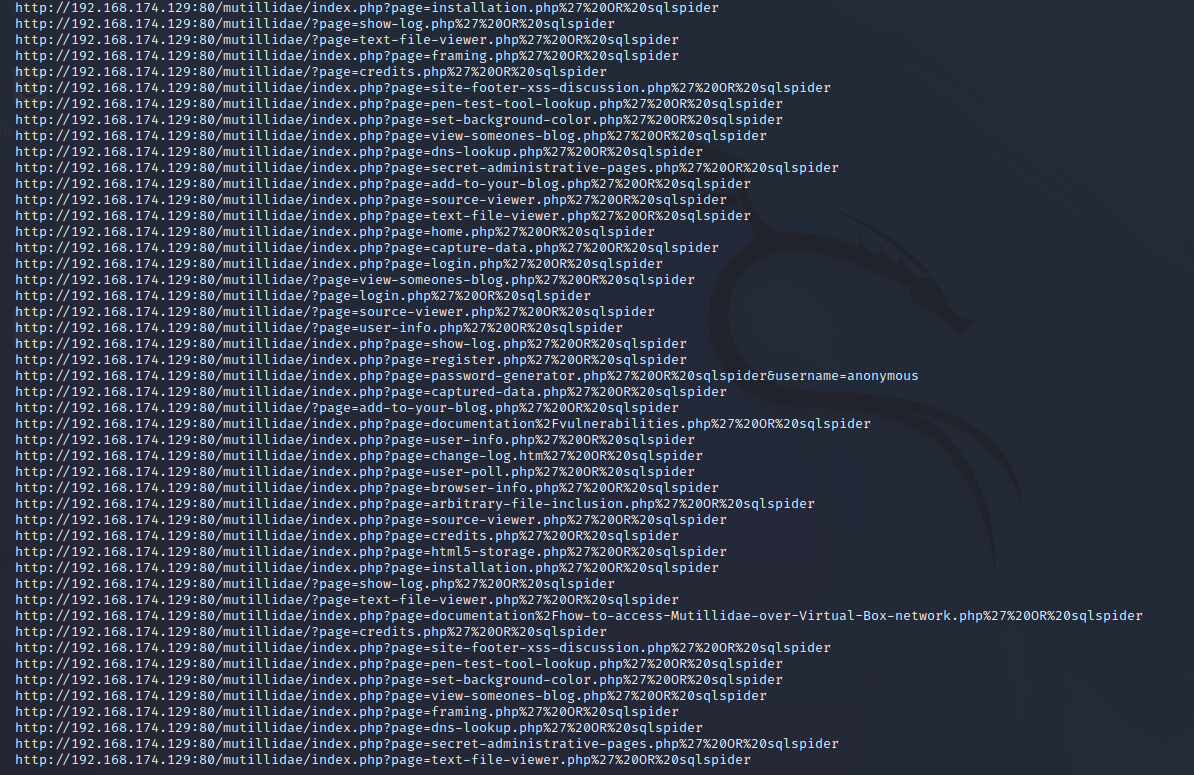


-Quét lỗ hổng bảo mật trên cổng 80 phía hệ thống victim:

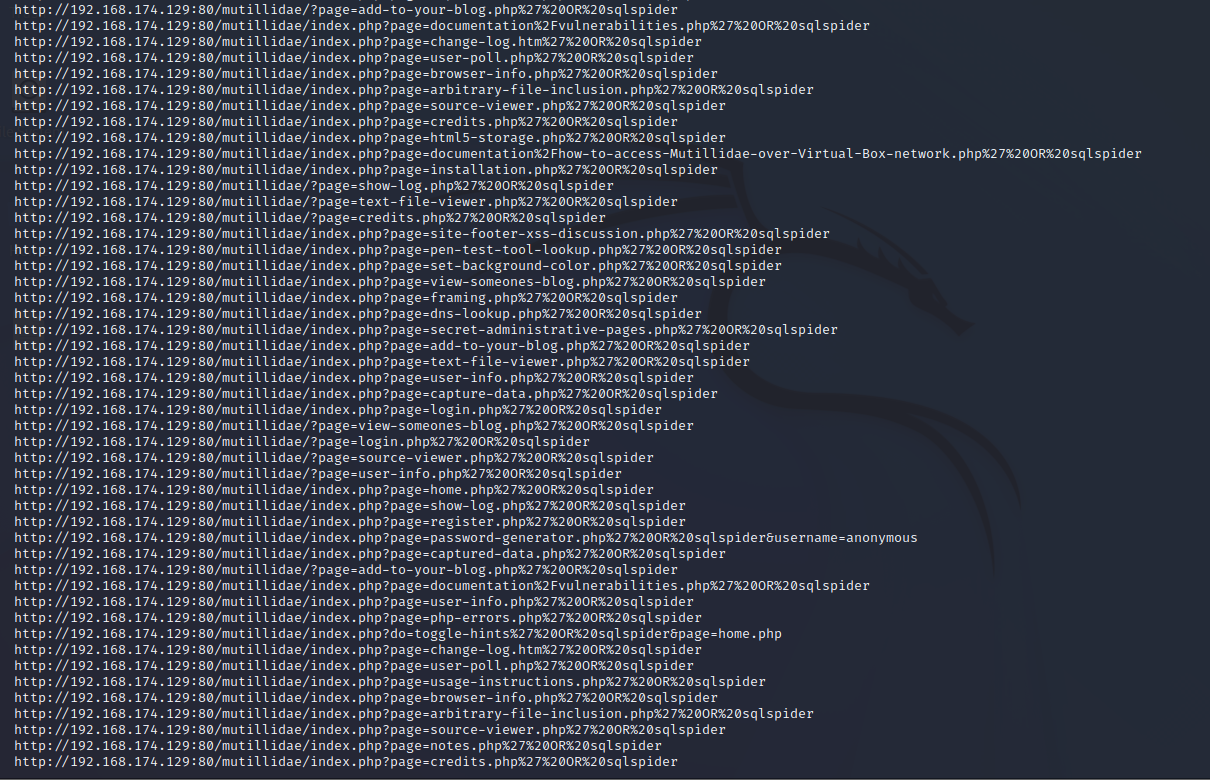
-> nmap -sV -sC --script=vuln -p 80 192.168.174.129

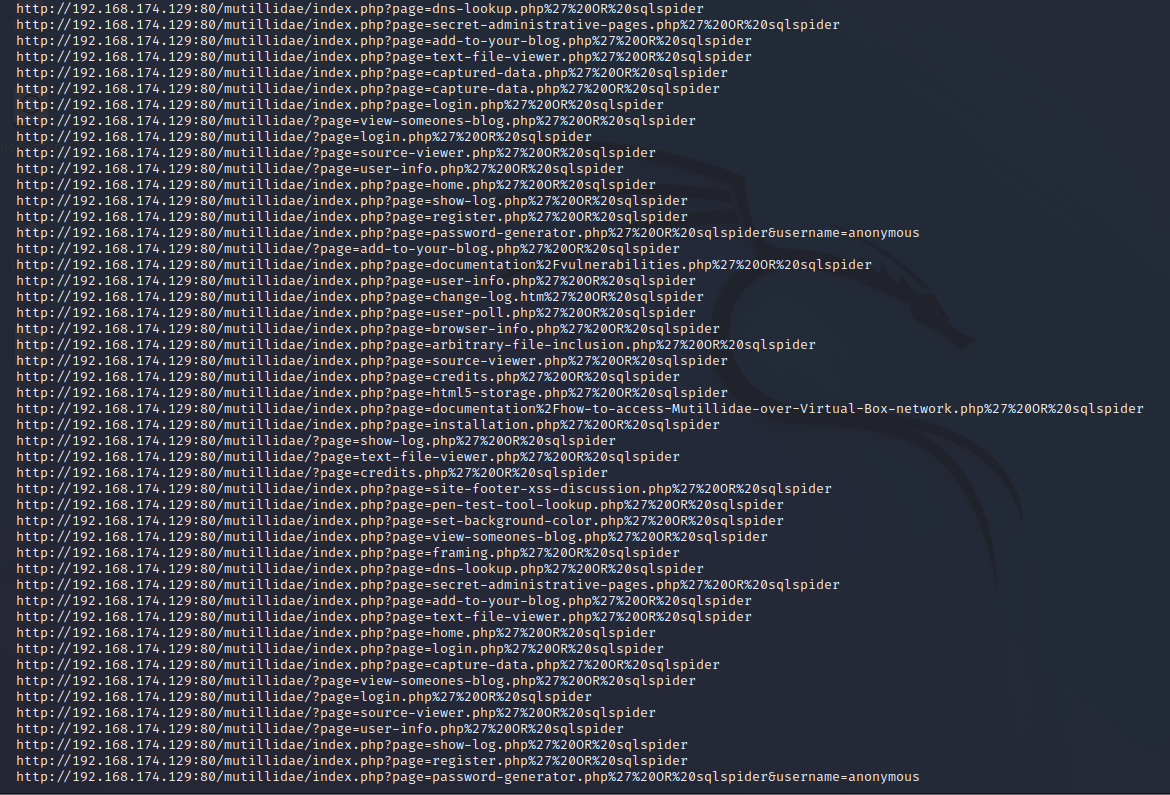


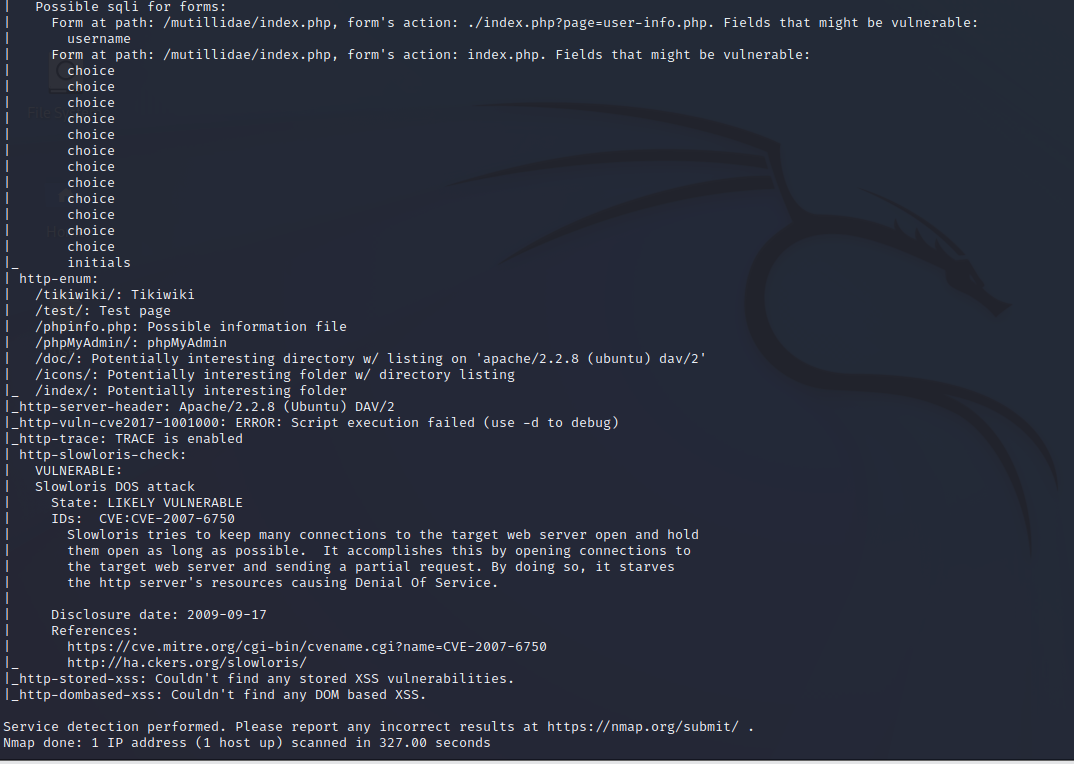






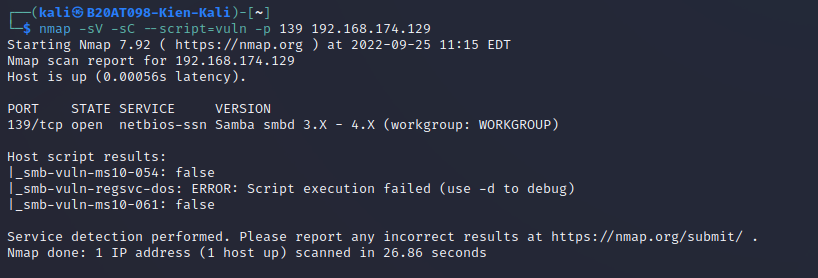






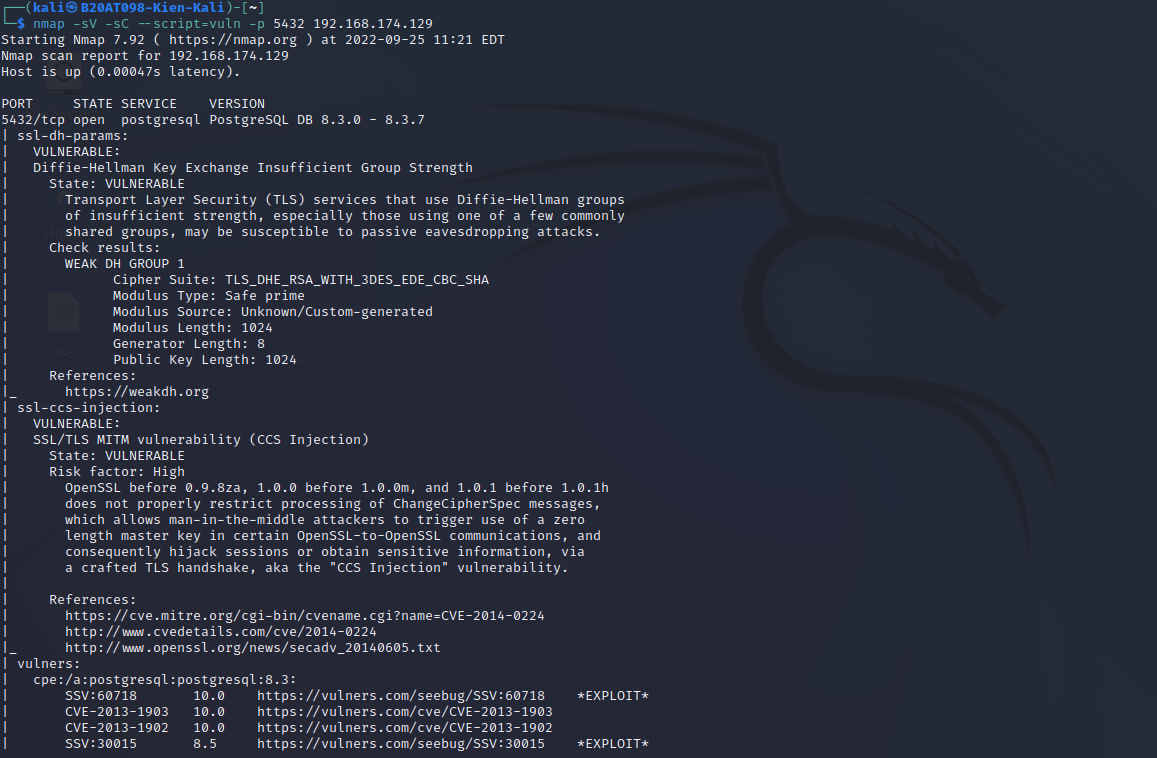
-Quét lỗ hổng bảo mật trên cổng 139 phía hệ thống victim:

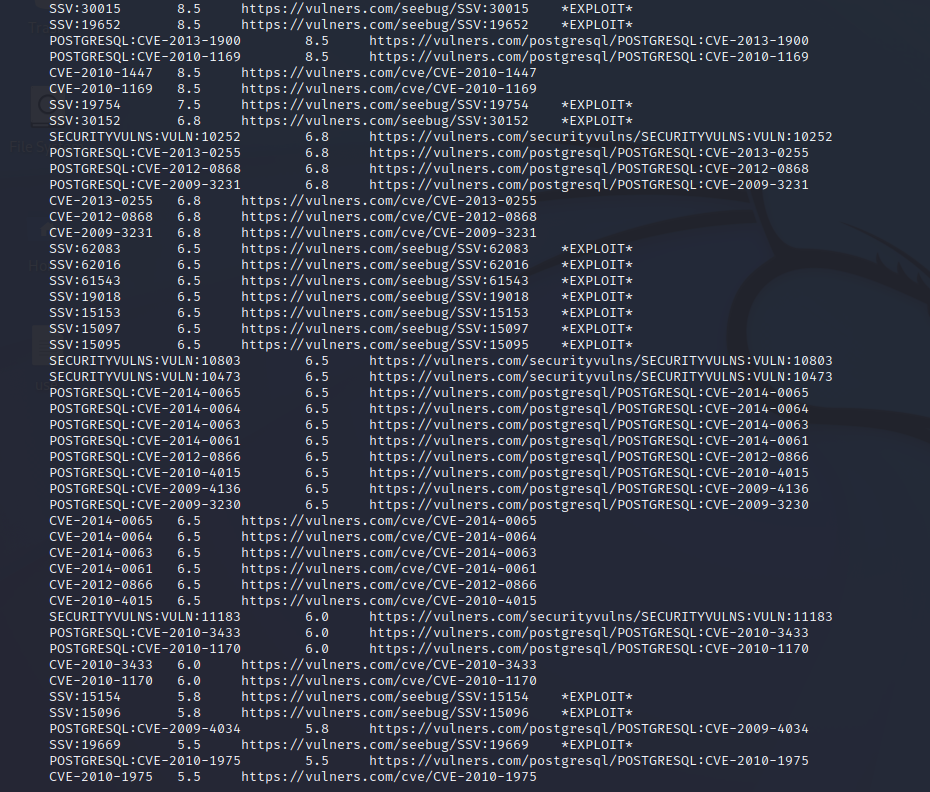
-> nmap -sV -sC --script=vuln -p 139 192.168.174.129



-Quét lỗ hổng bảo mật trên cổng 5432 phía hệ thống victim:

-> nmap -sV -sC --script=vuln -p 5432 192.168.174.129



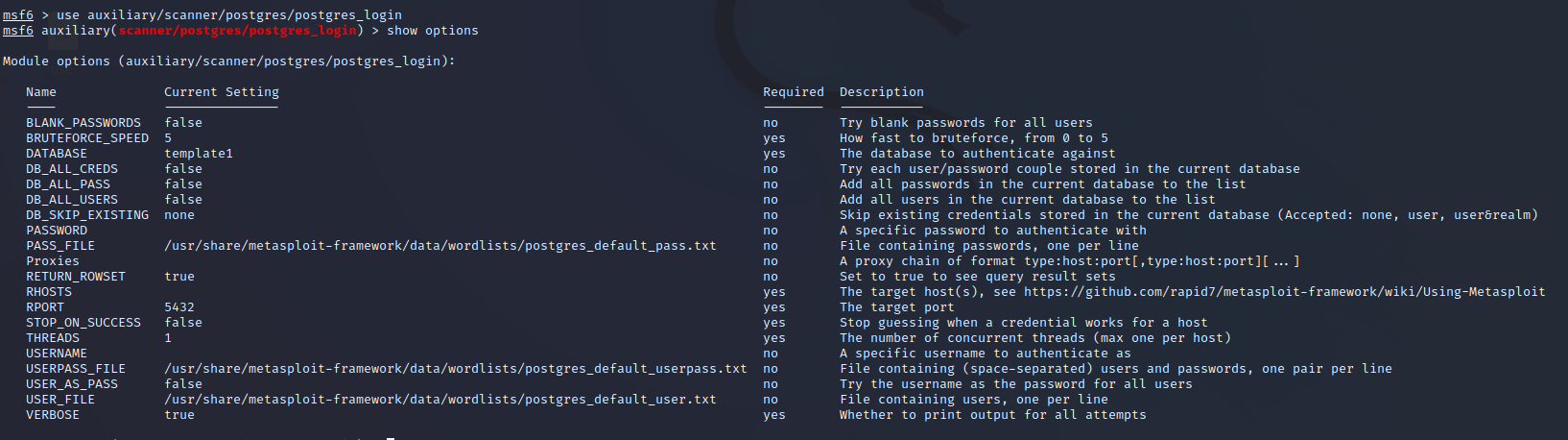




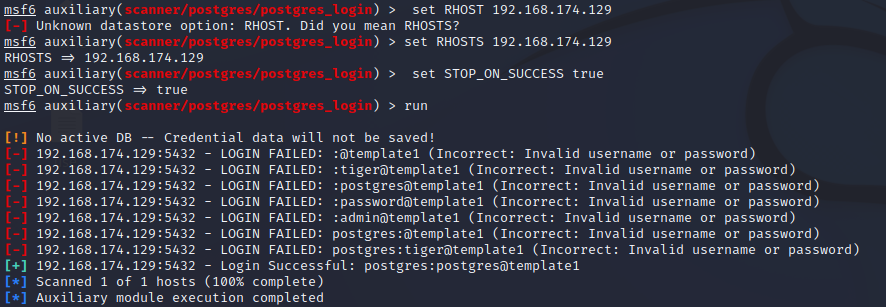
**4.Khai thác lỗi đăng nhập trên PostgreSQL, cổng 5432**

-Sử dụng module khai thác lỗi đăng nhập trên Postgres:

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



-Các tham số cần set RHOST , STOP\_ON\_SUCCESS :



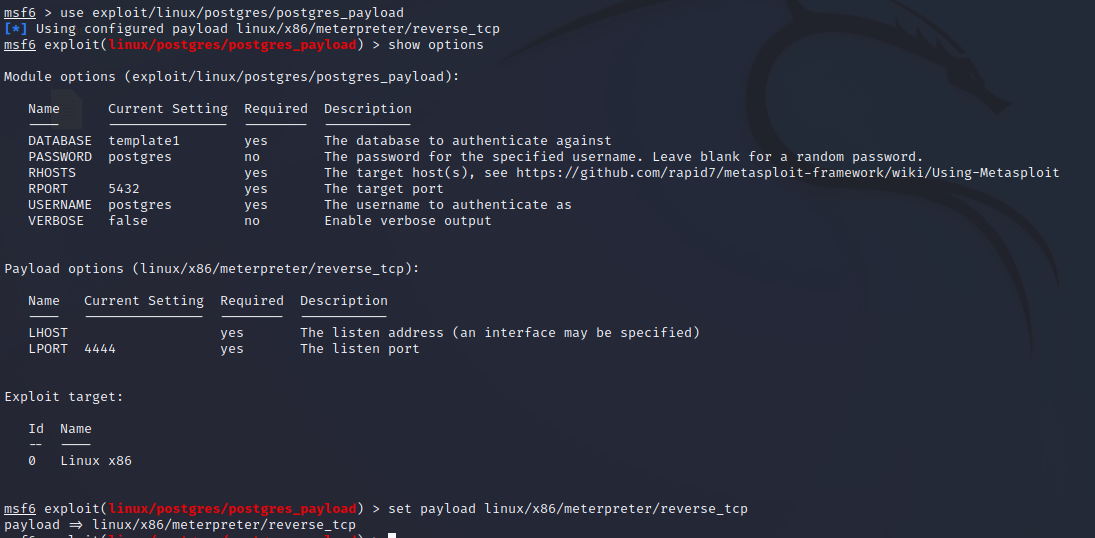
=>tài khoản đăng nhập vào dịch vụ CSDL phía victim được tìm ra sau quá trình tấn công: postgres@template1

**5.Khai thác lỗi trên PostgreSQL cho phép mở shell chạy với quyền root**

-Sau quá trình quét port 5432 bằng công cụ nmap , ta đã xác định được version của dịch vụ CSDL postgreSQL: PostgreSQL DB 8.3.0 - 8.3.7

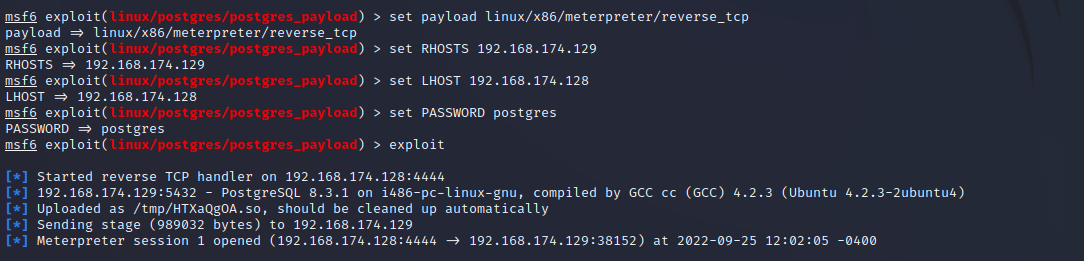


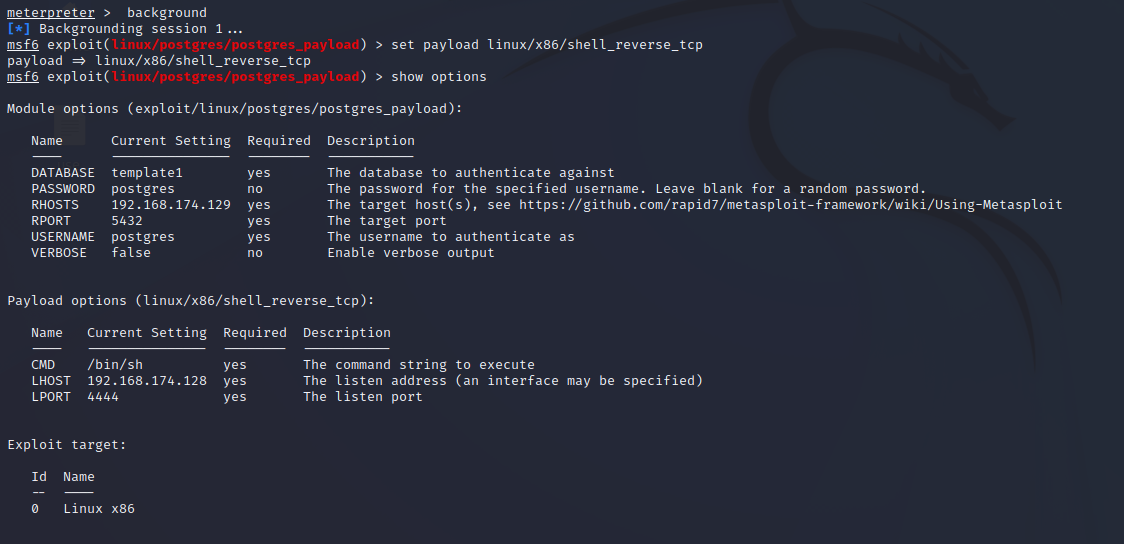
Sử dụng metaspolit dể tim module để khai thác phù hợp

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

-Sử dụng và setup cho module:

=>Có tất cả cần setup bao gồm : RHOSTS , LHOST , PASSWORD và USERNAME trong đó 2 tham số PASSWORD và USERNAME sẽ lần lượt thay bằng giá trị của username và password(postgres:postgres) ta đã tìm thấy thông qua quá trình brute-force trước đó.





-Kết thúc quá trình khai thác nhận được từ hệ thống:

