Trong bài, chúng ta sẽ khám phá phương pháp thực hiện cuộc tấn công vào máy chủ SQL Server. Qua việc sử dụng các công cụ và kỹ thuật thu thập thông tin, chúng ta có thể lấy được các dữ liệu quan trọng như thông tin đăng nhập của người dùng và cấu trúc của cơ sở dữ liệu. Điều này bao gồm việc xác định tên người dùng, mật khẩu, cũng như hiểu rõ về các bảng và quan hệ giữa chúng trong database.

Các bước thực hiện:

Bước 1:Máy window có Sql server:

A screenshot of a computer program

Description automatically generated

* Máy kali

A screenshot of a computer program

Description automatically generated

Bước 2:

-Để kiểm tra xem một máy có chạy dịch vụ SQL Server hay không, chúng ta có thể sử dụng nmap để quét port 1434, là port mặc định cho SQL Server Browser Service. Dịch vụ này có khả năng cung cấp thông tin hữu ích cho chúng ta, bao gồm việc xác định các thực thể của SQL Server đang hoạt động trên hệ thống mục tiêu.

A screenshot of a computer

Description automatically generated

A computer screen shot of a program

Description automatically generated

Phát hiện máy có chạy dịch vụ sql server

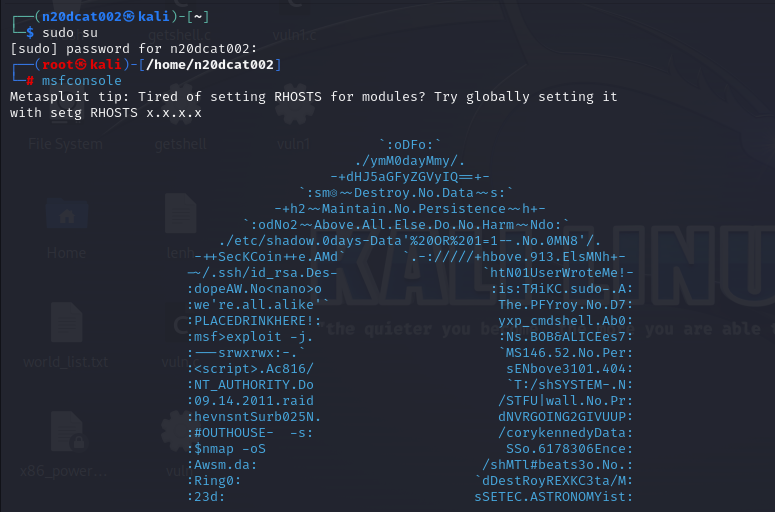
Bước 3:

Chúng ta sẽ triển khai Metasploit để thử nghiệm các mật khẩu cho tài khoản 'sa', dựa trên giả định rằng tài khoản này được bảo vệ bởi một mật khẩu yếu. Một khi đã xác định được mật khẩu, chúng ta có thể tiến hành đăng nhập và thu hoạch dữ liệu từ cơ sở dữ liệu.

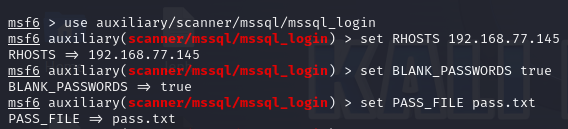
Chuẩn bị một tệp tin "pass.txt" bao gồm các mật khẩu được tạo ra một cách ngẫu nhiên nhưng dễ đoán.

A screenshot of a computer

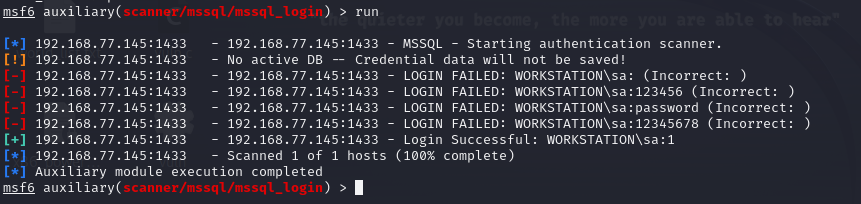
Description automatically generated  
-Gõ msfconsole



* Cấu hình cho Metasploit để bắt đầu dò mật khẩu



* Sau khi cấu hình xong ta bắt đầu chạy lệnh để dò mật khẩu



* Đã phát hiện thành công password cho tài khoản sa đó là **1**
* Tiếp tục cấu hình để cào dữ liệu database

**A screen shot of a computer

Description automatically generated**

* Chạy lệnh để lấy dữ liệu

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

-Như vậy, chúng ta đã thu thập thành công toàn bộ 100% thông tin đăng nhập của tài khoản 'sa' cũng như thông tin về các cơ sở dữ liệu mà tài khoản này có quyền truy cập.

Top of Form