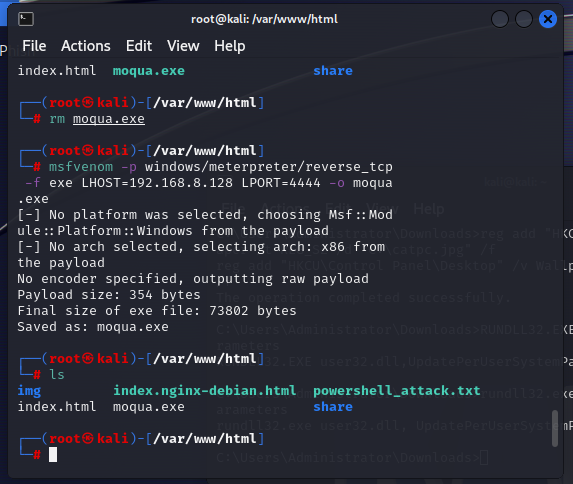
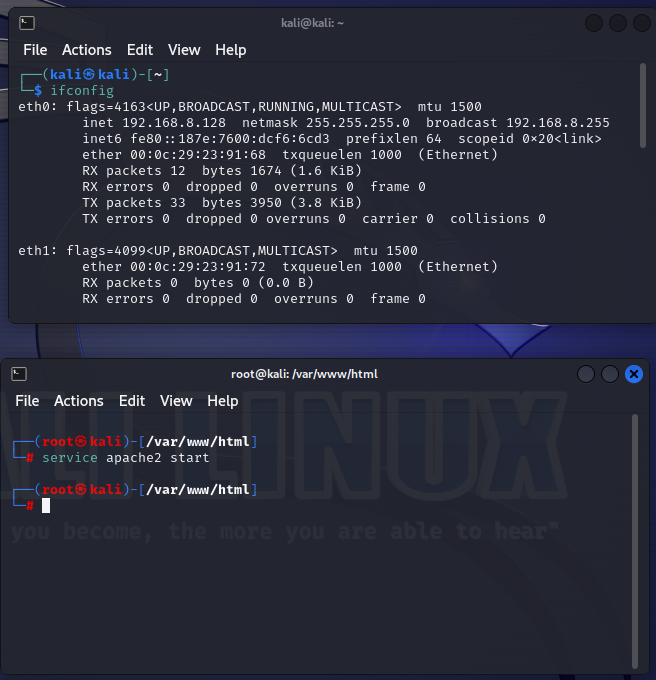
**Hack Windows 10 with msfconsole**

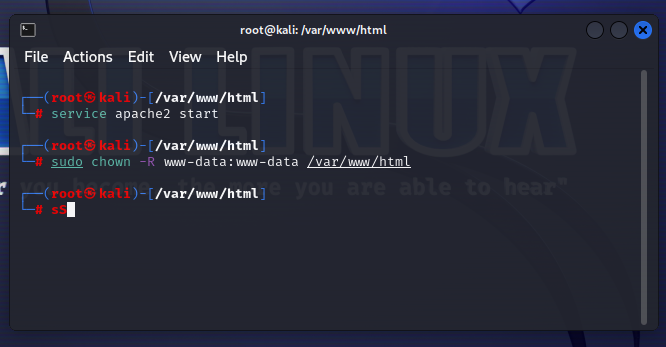
**Tạo file backdoor “moqua.exe” tại đường dẫn /var/www/html**



**Khởi động dịch vụ Apache HTTP**

****

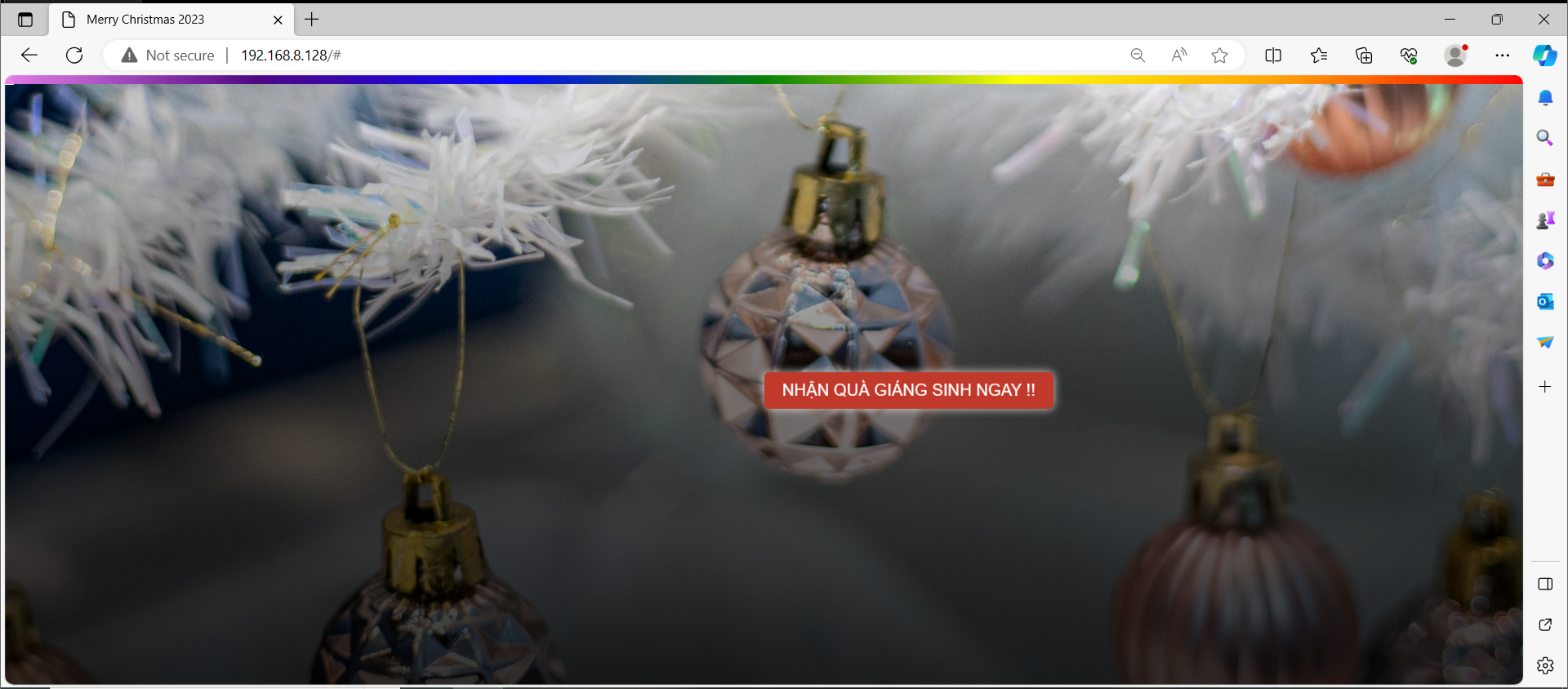
**Thay đổi quyền sở hữu của tất cả các tệp và thư mục con trong thư mục /var/www/html thành www-data:www-data**

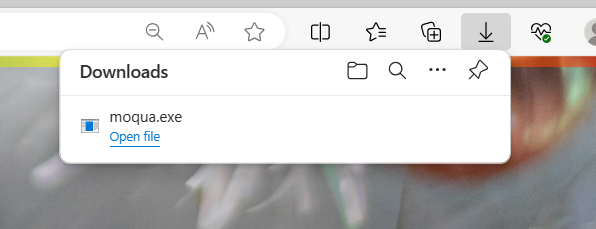
****

**Thay đổi quyền truy cập của tất cả các tệp và thư mục con trong thư mục /var/www/html thành 755**

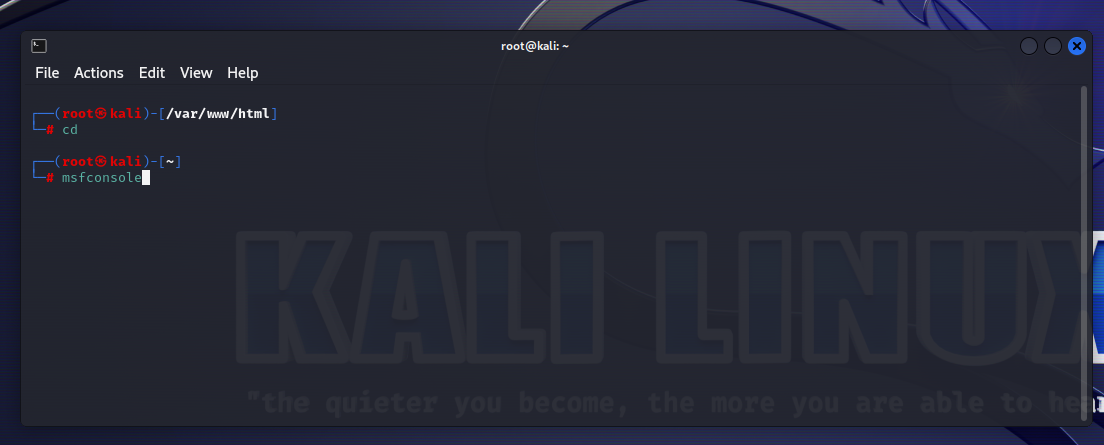
****

**Tạo 1 trang website giả, khi victim nhấn vào button thì sẽ tải file backdoor về**

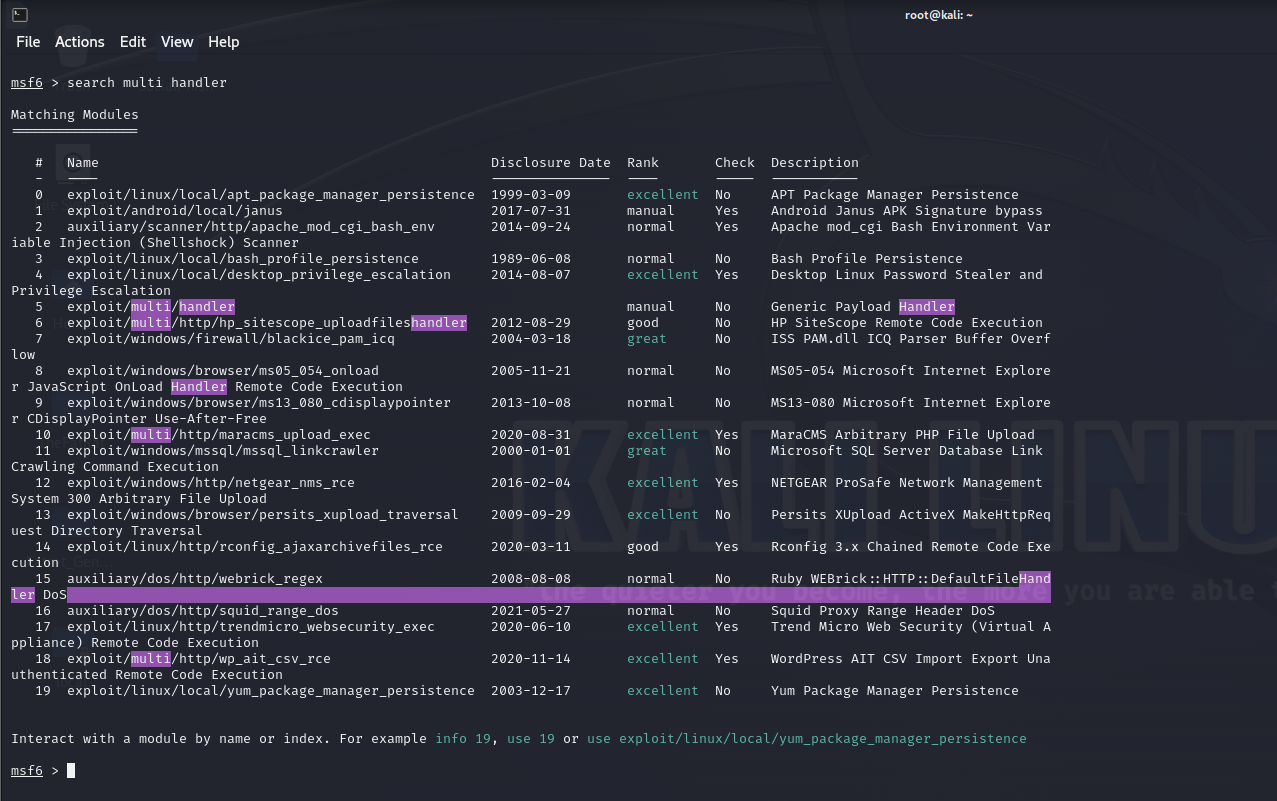
****

****

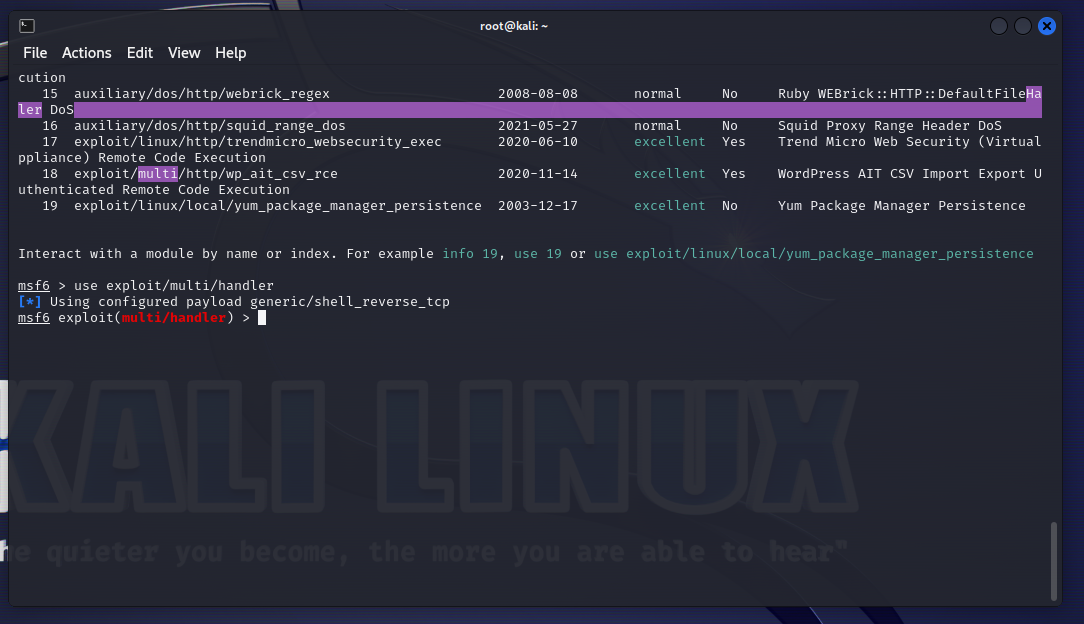
**Tiếp theo vào msfconsole**

****

**Tìm kiếm các payloads Metasploit có thể được sử dụng để tạo một handler đa mục tiêu**

****

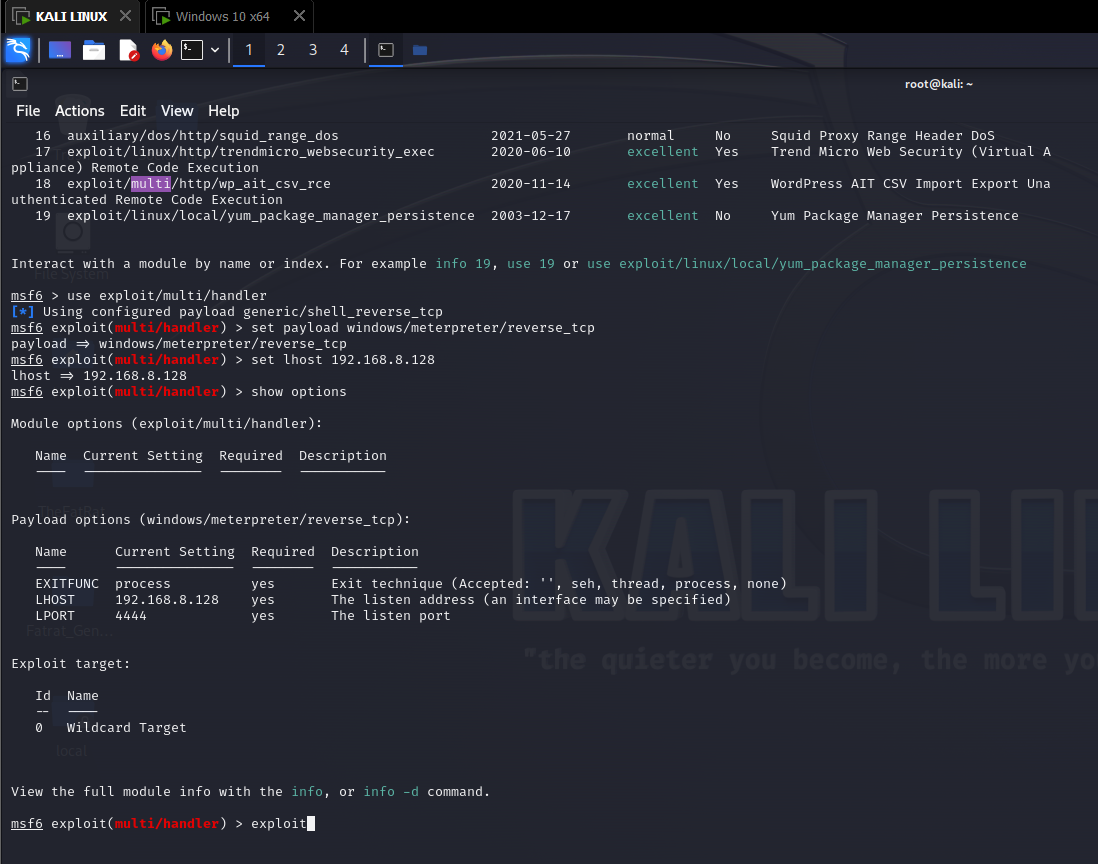
**Sử dụng payload *exploit/multi/handler* Metasploit để tạo một handler đa mục tiêu**

****

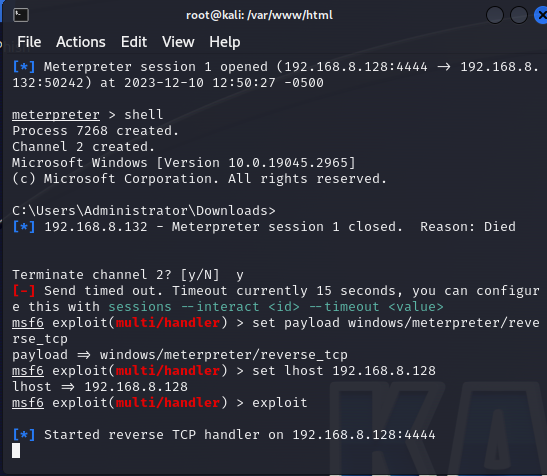
Cấu hình payload

set lhost máy kali

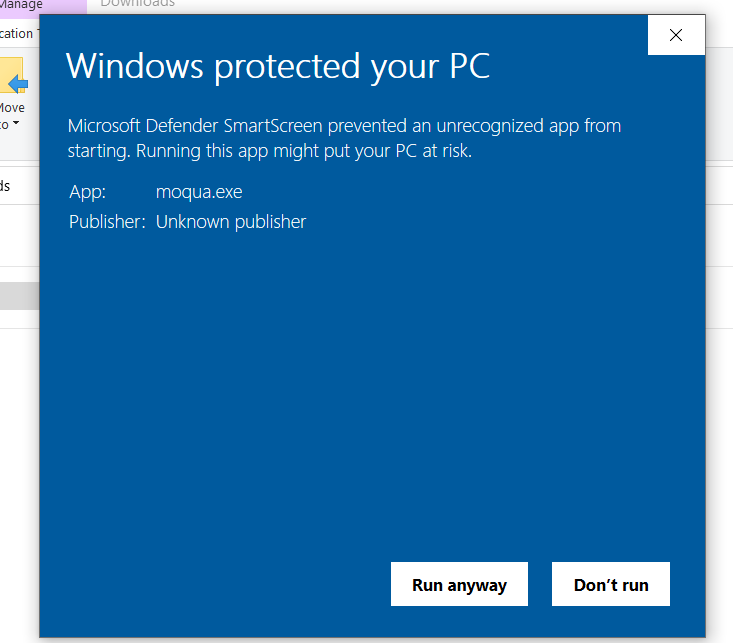
Sử dụng exploit để chạy các cấu hình đã được triển khai

****

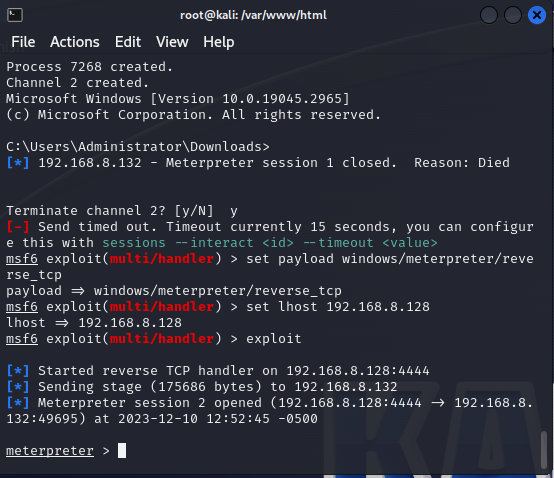
**Lúc này sẽ trong trạng thái chờ kết nối**

****

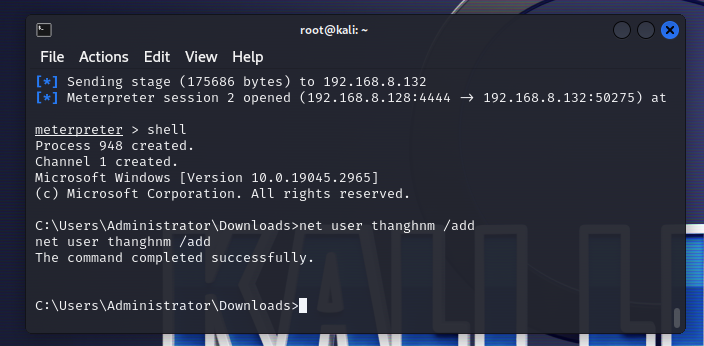
**Khi victim mở file backdoor “moqua.exe” thì sẽ mở 1 kết nối ngược tới máy kali**

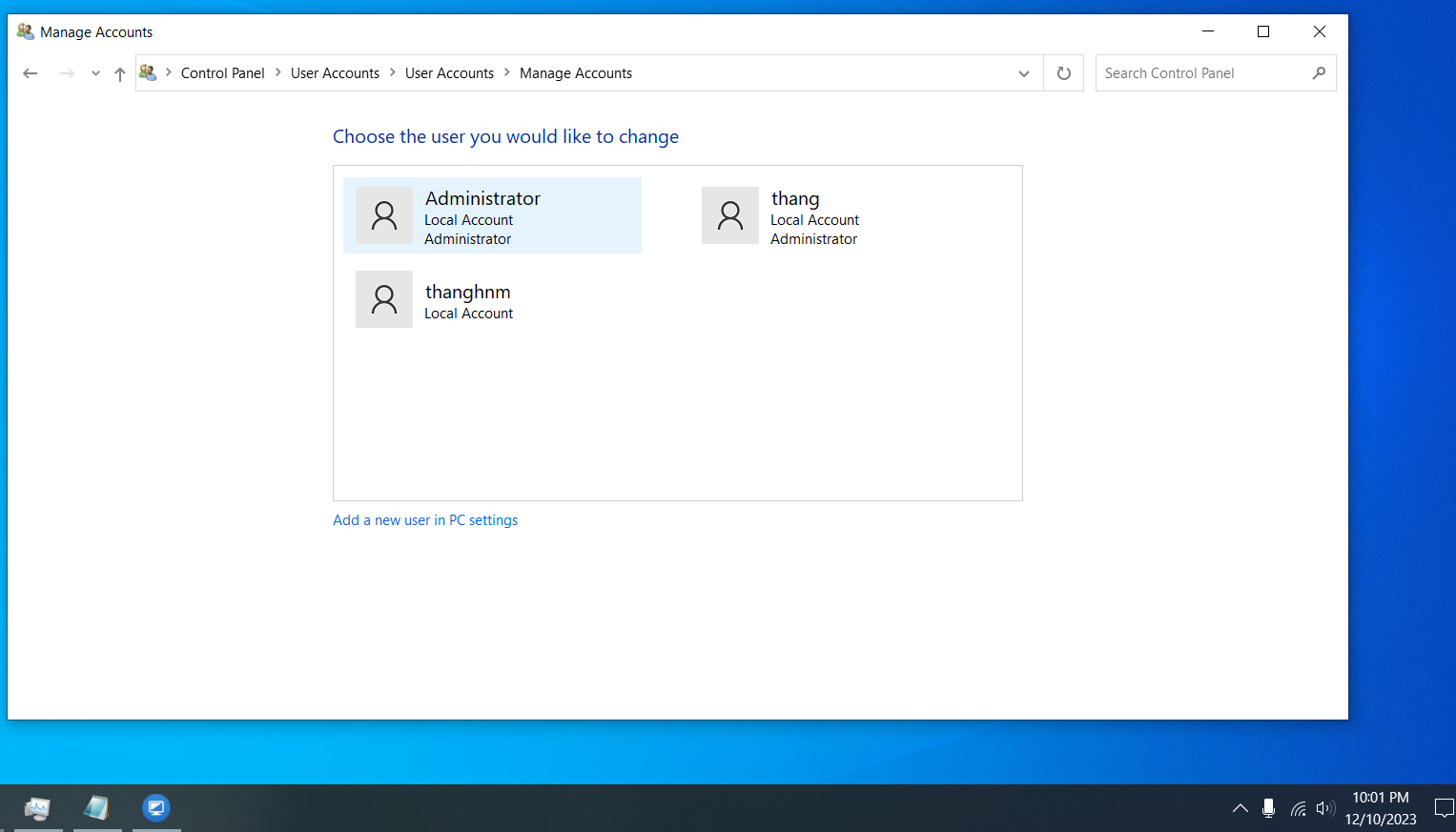
****

**Sau khi victim chạy backdoor, lúc này máy kali đã xâm nhập thành công máy victim**

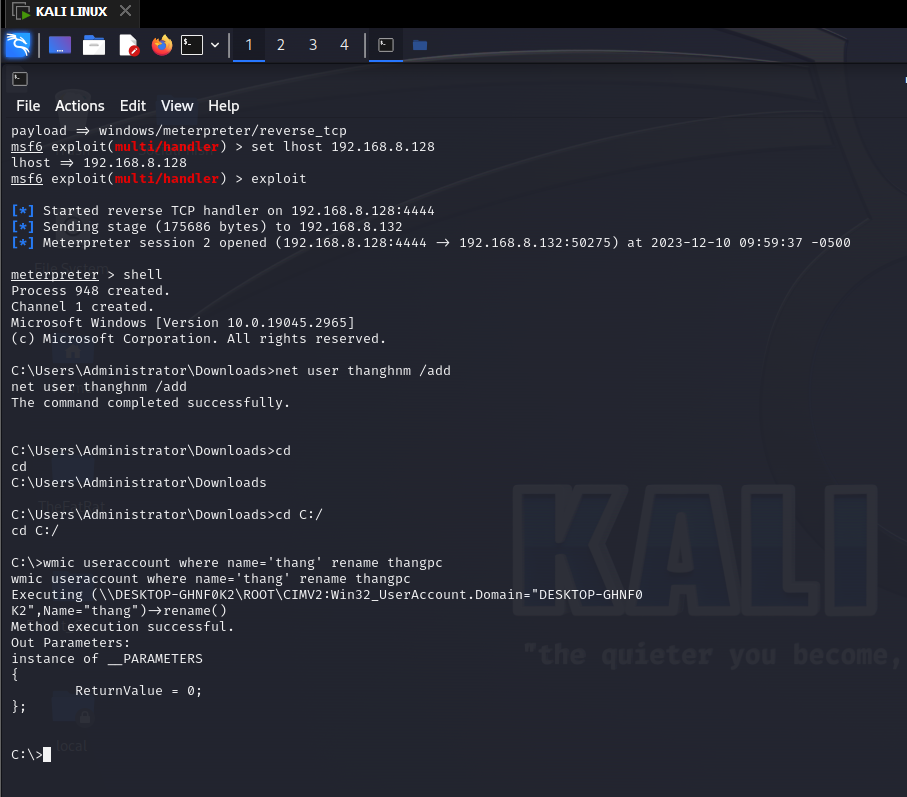
****

**Tạo thử 1 user bất kì tại máy victim**

****

****

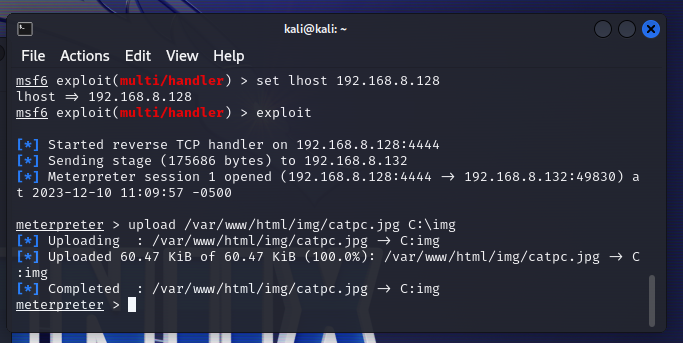
**Đổi tên user gốc “thang” thành “thangpc”**

****

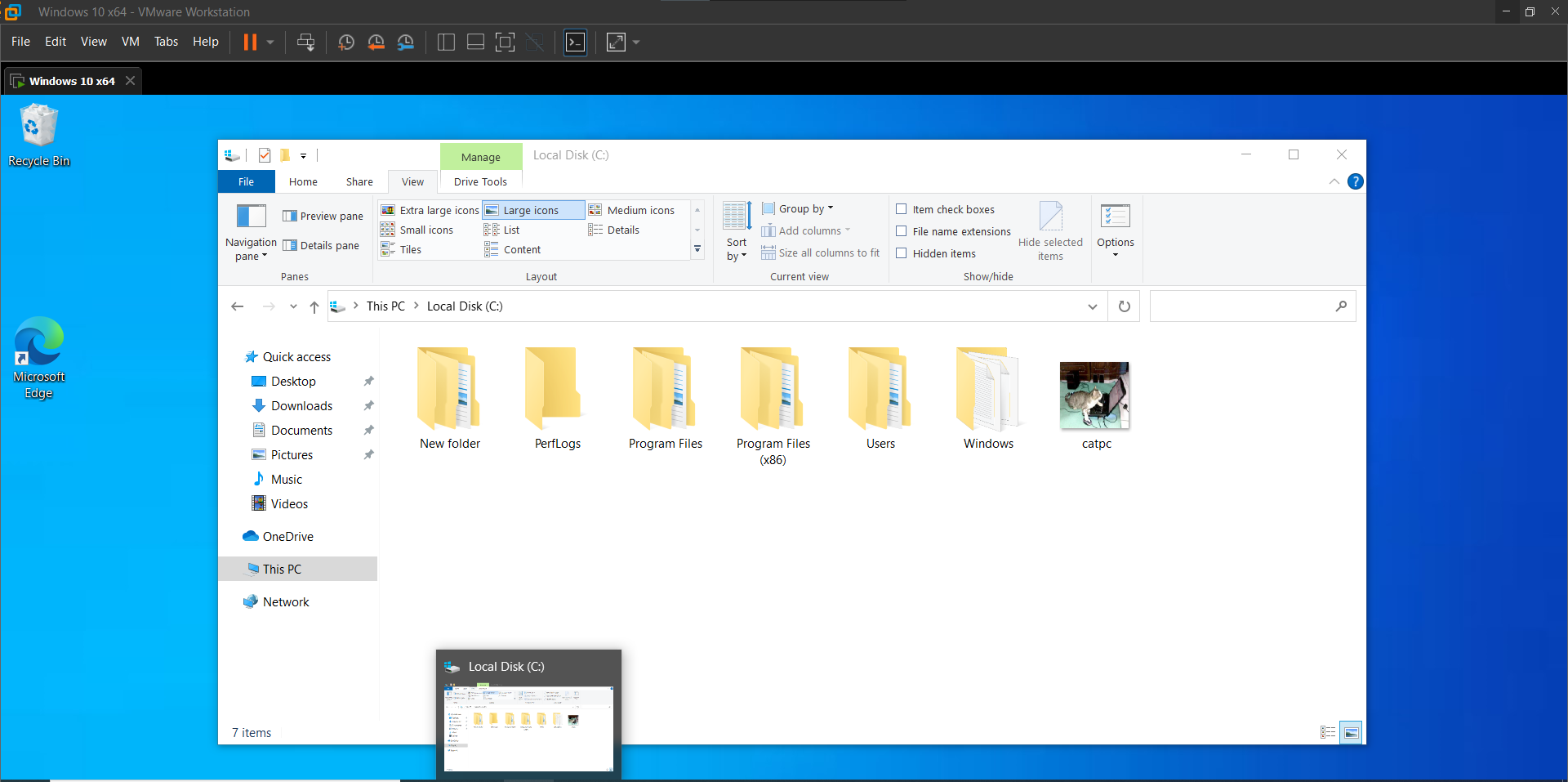
****

**Đổi hình nền của máy victim**

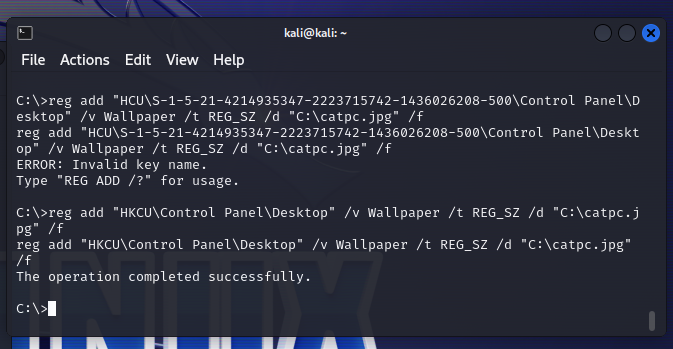
**Tại meterpreter, copy hình đã chuẩn bị vào ổ C của máy victim**

****

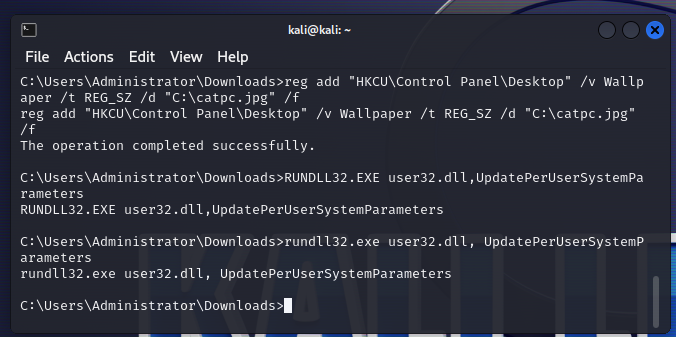
**Thành công**

****

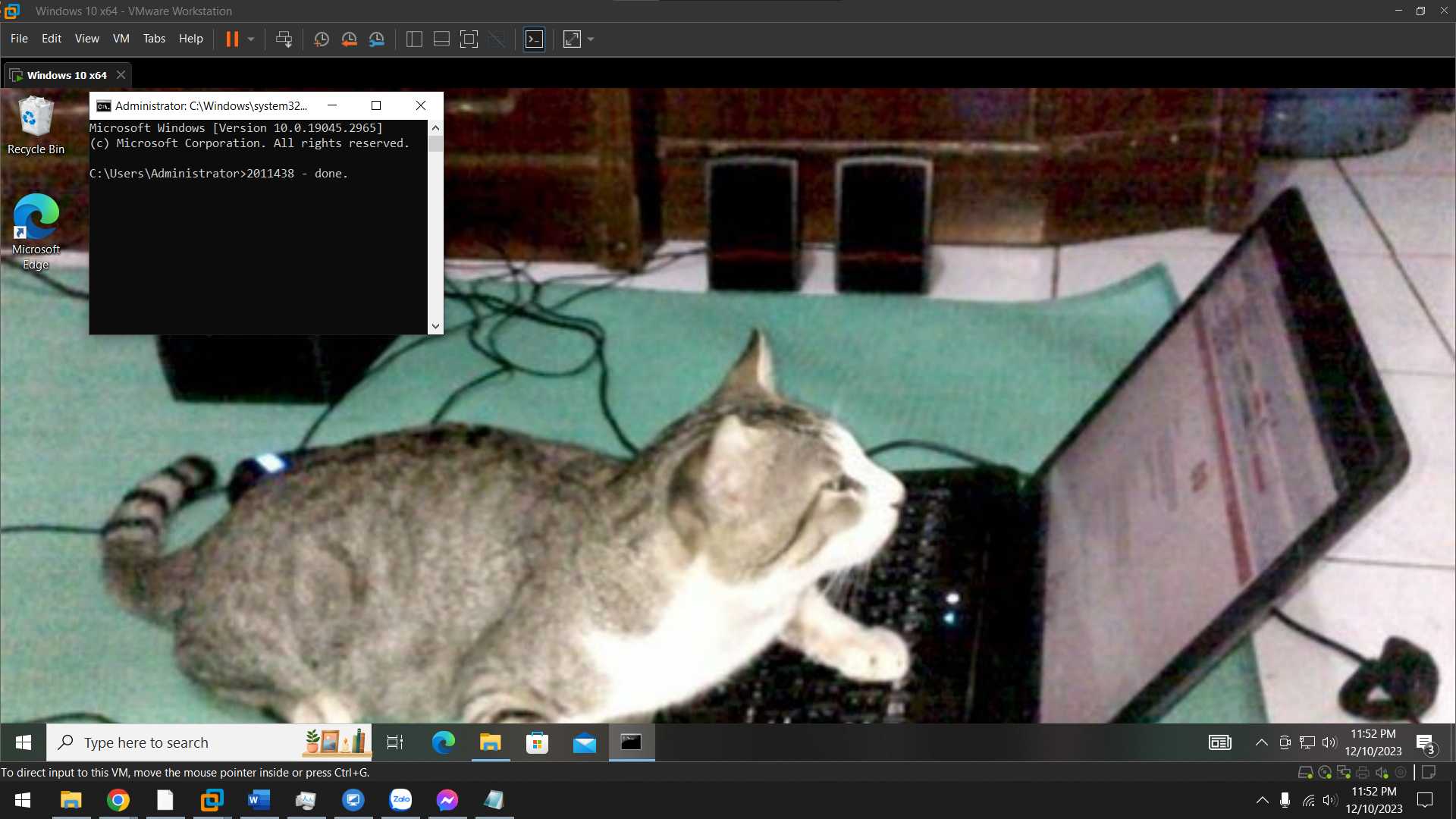
**Tiến hành đổi hình nền tại máy victim thuộc user “Administrator” thông qua Registry**

****

**Sử dụng lệnh *rundll32.exe user32.dll, UpdatePerUserSystemParameters* để làm mới màn hình của victim**

****

**Lúc này hình nền của victim đã bị hack**

****

**Video:**[**https://www.youtube.com/watch?v=V0lV4dhgNiU&list=PLVMR1gJ1n0YB2aQfUoxpXqTSuhsAZL30r&index=2**](https://www.youtube.com/watch?v=V0lV4dhgNiU&list=PLVMR1gJ1n0YB2aQfUoxpXqTSuhsAZL30r&index=2)