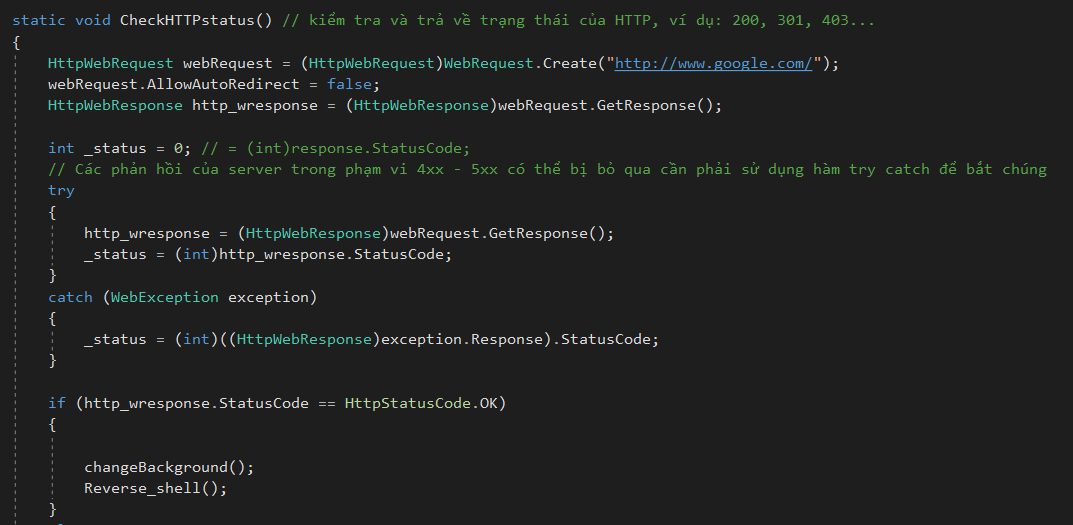
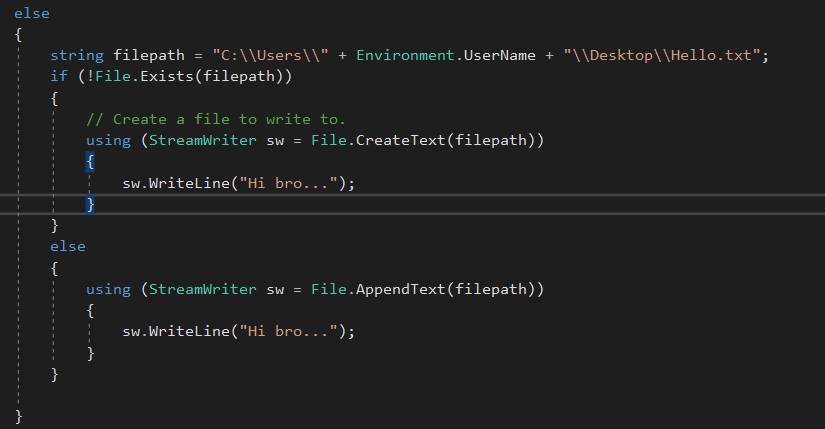
3.



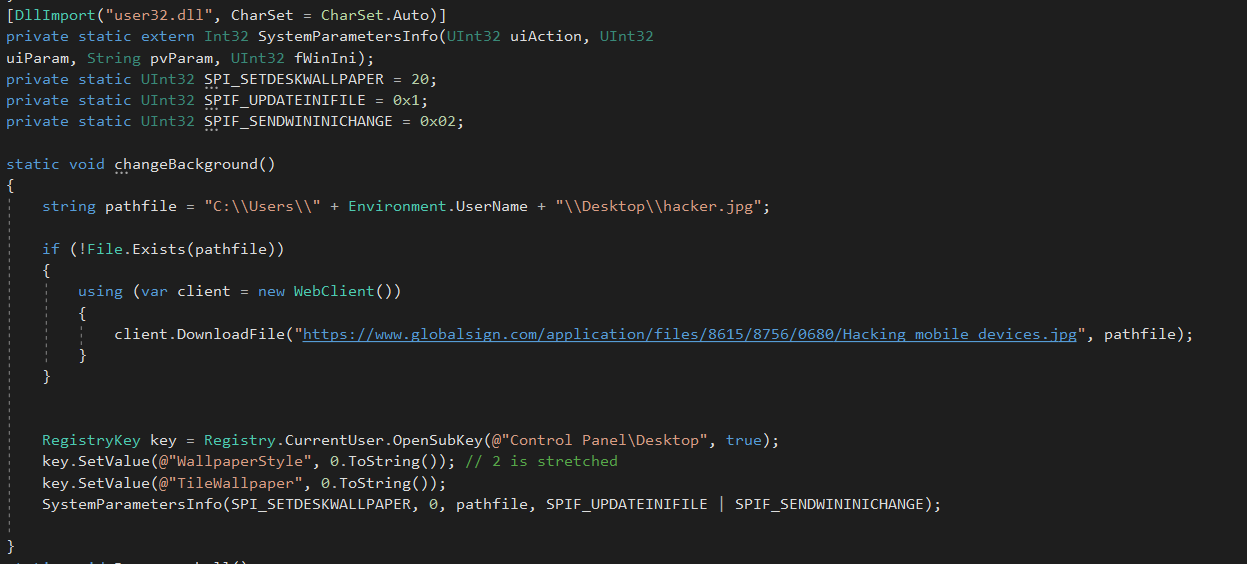
Hình 3.1 Kiểm tra tình trạng internet.

Sử dụng GetResponse() để lấy trạng thái trang web, trả về trạng thái 200 tức máy tính hiện tại có thể truy cập internet.

Khi có internet sẽ tiến hành thay đổi hình nền và thực hiện reverse shell.Ngược lại sẽ tạo file “Hello.txt” ở desktop .



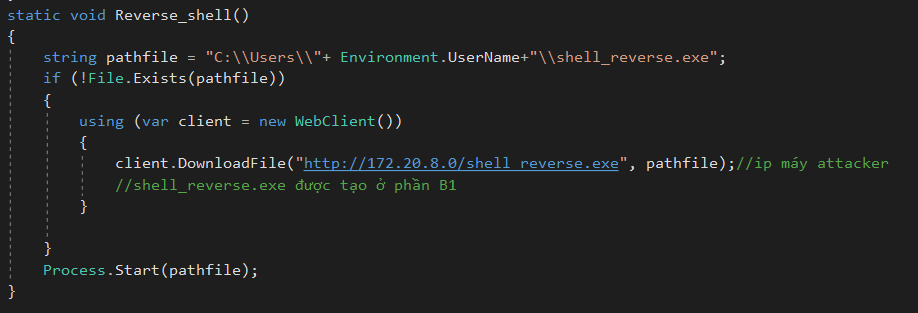
Hình 3.2 Tạo file ở Desktop.



Hình 3.3 Thay đổi hình nền.

Kiểm tra file ảnh đã tồn tại trong máy hay chưa, nếu chưa thì tiến hành tải file.

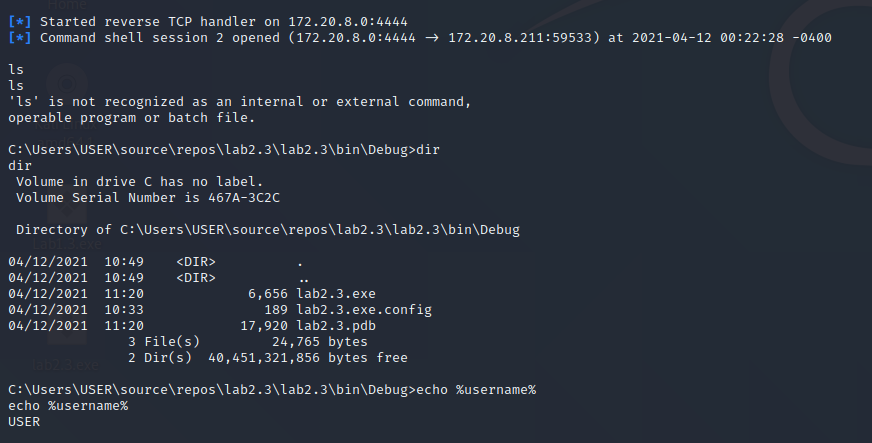
Tiến hành cập nhật Registry để chọn “Fit style” cho hình nền. Sử dụng lệnh “SystemParametersInfo” để thay đổi hình nền.



Hình 3.4 Thực hiện Reverse shell.

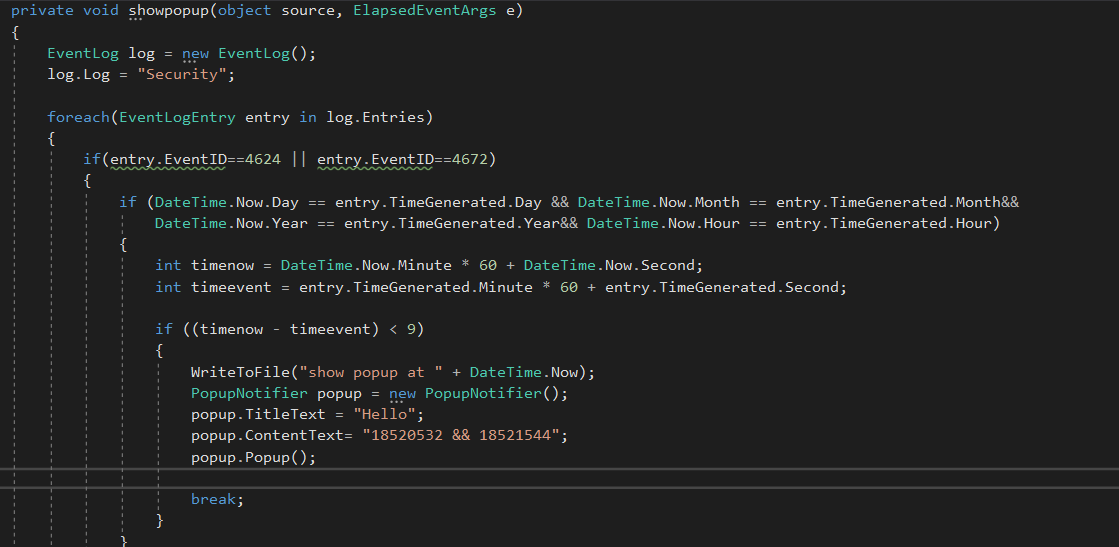
Kiểm tra file shell\_reverse.exe đã tồn tại hay chưa, nếu chưa thì tải file về ( file này đã được tạo ở phần trước).

Sau khi đã có file tiến hành thực thi file để kết nối đến máy attacker.



Hình 3.5 Kết quả.

4.



Hình 4.1 Hiện popup khi logon.

Để xác định người dùng logon thành công cần kiểm tra trong Eventlog với ID của event này là 4624 hoặc 4672. Vì chỉ xuất hiện popup 1 lần nên ta cần kiểm tra lần logon lần cuối cùng có phải vừa logon thành công hay không.