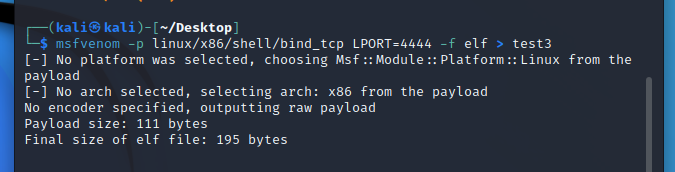
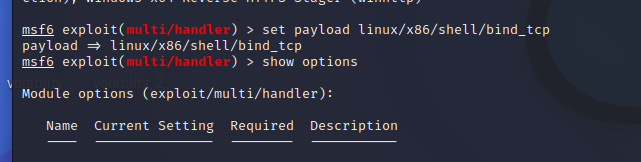
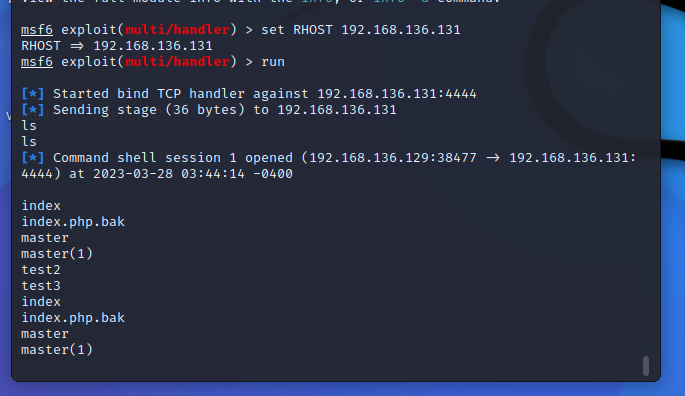
1. Thực hiện tạo payload khác (không phải reverse TCP) có thể chạy trên hệ điều hành Linux



* Tạo payload



* Set payload linux/x86/shell/bind\_tcp





* Thực thi lệnh trên máy

2. Có 2 loại payload trên Metasploit Framework là Staged và Non-Staged. Hãy tạo ra reverse shell cho từng loại

- Staged payload yêu cầu tải xuống mã thực thi bổ sung từ máy chủ Metasploit để hoàn thành reverse shell

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Tạo reverse shell cho stage payload

Ảnh có chứa văn bản

Mô tả được tạo tự động

- Thực hiện exploit

Ảnh có chứa văn bản, ngoài trời, ảnh chụp màn hình, tấm biển

Mô tả được tạo tự động

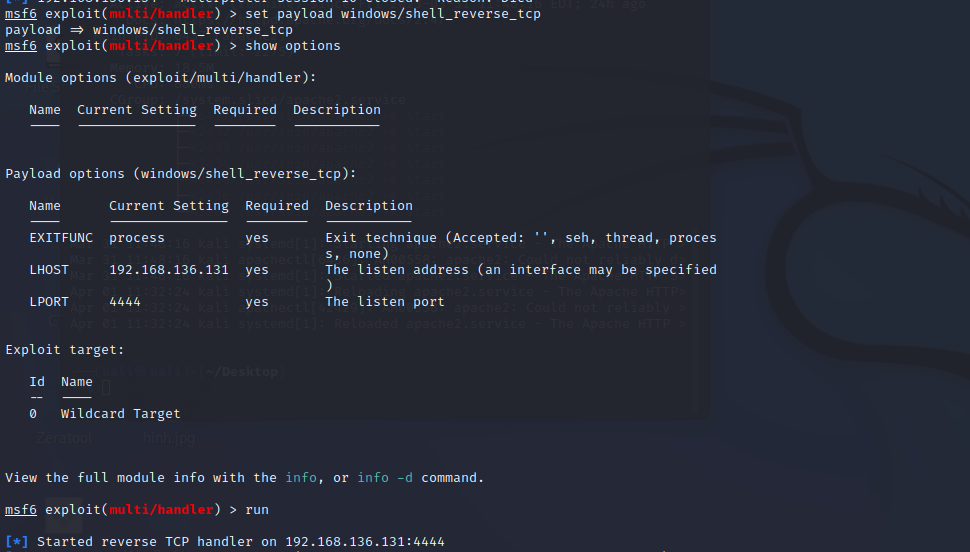
- Kết quả exploit

- Non-stage payload có thể thực thi 1 lần để tạo reverse shell mà không cần tải xuống bất kỳ mã nào từ máy chủ Metasploit

Ảnh có chứa văn bản

Mô tả được tạo tự động

- Tạo file reverse shell cho non-stage payload



- Thực hiện exploit

Ảnh có chứa văn bản

Mô tả được tạo tự động

- Kết quả exploit

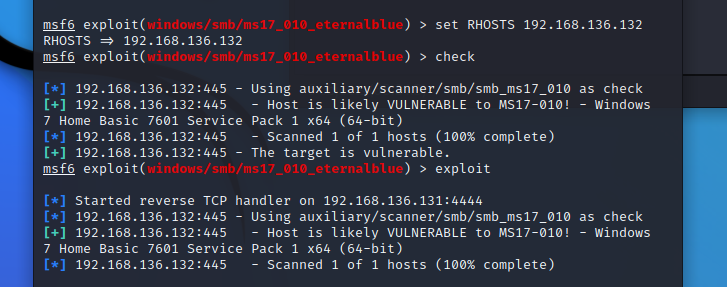
- So sánh

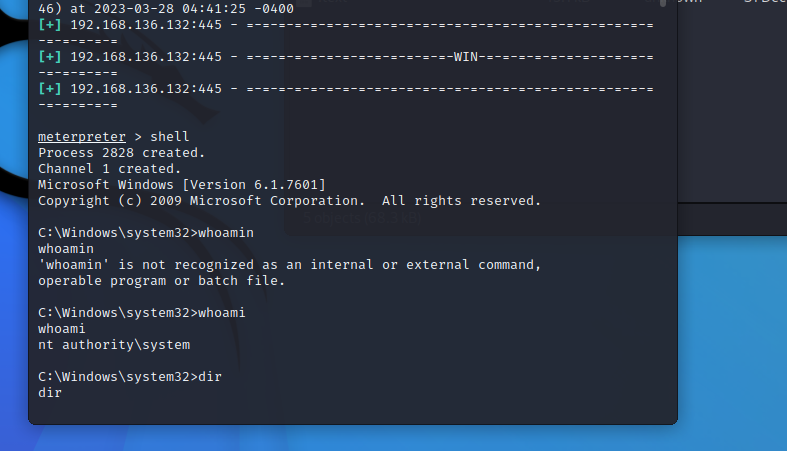
|  |  |  |
| --- | --- | --- |
|  | Staged payload | Non-staged payload |
| Kích thước | ó kích thước nhỏ hơn Non-Staged payload, do Staged  Payload chỉ gửi một stager nhỏ đến máy nạn nhân, stager này có nhiệm vụ kết nối ngược lại đến  máy attacker và download các phần payload cần thiết | Có kích thước lớn, do Non-Staged Payload gửi toàn bộ payload cần thiết đến máy nạn nhân chỉ trong một lần duy nhất,  vì vậy nó không yêu cầu  attacker cung cấp thêm bất kì dữ liệu nào nữa |
| Công cụ lắng nghe | Do Stage payload cần download thêm các payload khác từ attacker nên nó cần 1 bộ công cụ  lắng nghe đặc biệt như  multi/handler trong Metasploit. | Do đơn giản hơn Stage Payload, nên Non-Stage Payload có thể sử dụng nhiều công cụ lắng nghe khác nhau, như Netcat. |
| Khả năng phát hiện của các trình anti-virus | Khó phát hiện hơn so với Non-Stage Payload, do có kích thước nhỏ -> dễ che dấu | Dễ bị phát hiện |

5. So sánh giữa việc viết virus bằng dịch vụ trên C# so với việc tạo bằng MSF (quyền, khả năng phát hiện, …)

|  |  |  |
| --- | --- | --- |
|  | Window Service C# | MSF |
| Quyền truy cập | Cho phép ta có toàn quyền kiểm soát đối tượng được tạo ra. Có thể tùy chỉnh virus để phù hợp với nhu cầu | Có thể bị giới hạn 1 số tính năng và lựa chọn do khả năng của MSF |
| Khả năng phát hiện | Khó phát hiện hơn do tùy chỉnh virus để tránh bị phát hiện bởi các phần mềm anti-virus | Dễ bị phát hiện vì sử dụng các payload phổ biến và rộng rãi bởi các hacker |
| Khả năng tấn công | Cho phép thực hiện tấn công vào 1 dịch vụ hoặc hệ thống cụ thể | Sử dụng các lỗ hổng đã biết và các công cụ phát hiện lỗ hổng để thực hiện các cuộc tấn công |

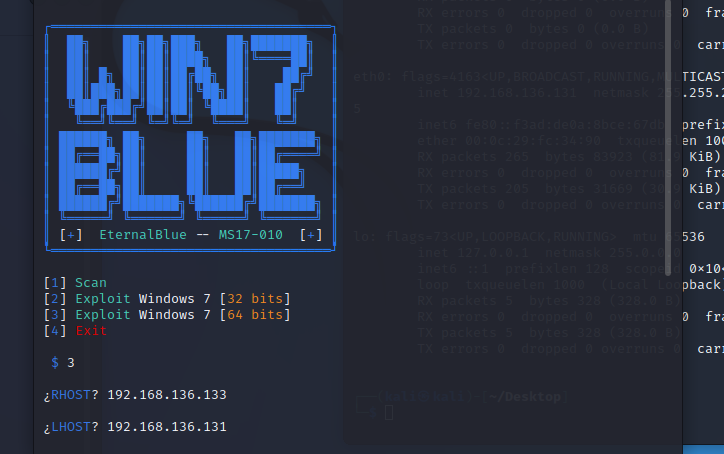
B.2.1 Khai thác lỗ hổng MS17-010 sử dụng Metasploit





B.2.2 Khai thác lỗ hổng MS17-010 không sử dụng Metasploit

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động