***Lưu ý****: Vì đây là mô phỏng nên những phần như recon để biết xem protocol có hoạt động không thì mình sẽ lược bỏ bớt. (vì do mình cấu hình tạo ra nó mà mà hehe)*

**1️ Chuẩn bị Target VM (Windows 11 + Outlook)**

**a) Tạo VM Windows 11**

1. **VirtualBox hoặc VMware**: tạo một VM mới.
2. **Cấu hình cơ bản**:
   * RAM: 4–8 GB
   * CPU: 2 cores trở lên
   * Disk: 60–100 GB
   * Network adapter: Host-Only Adapter (chỉ giao tiếp với attacker VM)
3. **ISO Windows 11**: mount ISO để cài đặt.

**b) Cài đặt Windows 11**

1. Chạy Windows 11 installer trên VM.
2. Tạo user admin để thử exploit.
3. Tắt Windows Update trong VM để giữ phiên bản Outlook/Windows chưa patch lỗ hổng.
4. Bật SMBv1 nếu cần (một số PoC cũ có thể yêu cầu).

**c) Cài Microsoft Outlook**

1. Cài phiên bản Outlook tương thích với CVE-2023-23397 (ví dụ Outlook 2019/2021 hoặc Outlook trong Office 365 build cũ).
2. Test Outlook hoạt động bình thường bằng cách gửi/nhận email nội bộ.

**d) Tạo snapshot “vulnerable\_clean”**

* Trên VMware/VirtualBox: **Snapshot → Create Snapshot**
* Snapshot này sẽ giúp bạn revert về trạng thái sạch sau khi thử PoC.

**2️ Chuẩn bị Attacker VM (Kali Linux)**

**a) Tạo VM Kali Linux**

1. RAM: 4 GB, CPU: 2 cores.
2. Network adapter: cùng Host-Only network với target.

**b) Cài đặt tool cần thiết**

sudo apt update

sudo apt install responder python3-impacket

 responder → dùng để capture NTLM hash.

 impacket → dùng ntlmrelayx.py để thực hiện relay.

**c) Gán IP tĩnh**

*sudo ip addr add 192.168.1.2/24 dev eth0*

*sudo ip route add default via 192.168.1.1 (thực ra cũng không cần lắm vì mình cắm dây cho 2 máy để cho nhanh luôn mà)*

Ví dụ:

* Attacker: 192.168.1.2
* Target: 192.168.1.3 *(còn trên windows thì mình dùng interface để chỉnh)*

**3️ Kiểm tra kết nối mạng**

Trên Target:

ping 192.168.1.2

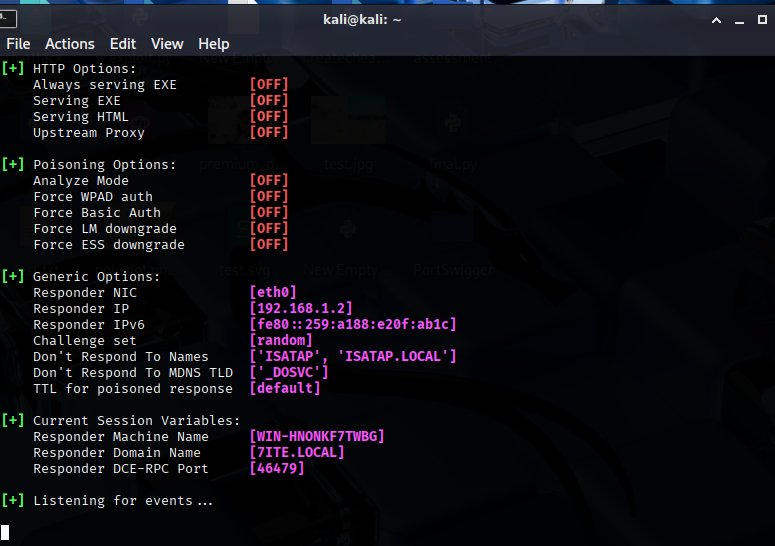
Nếu ping được → network lab hoạt động.

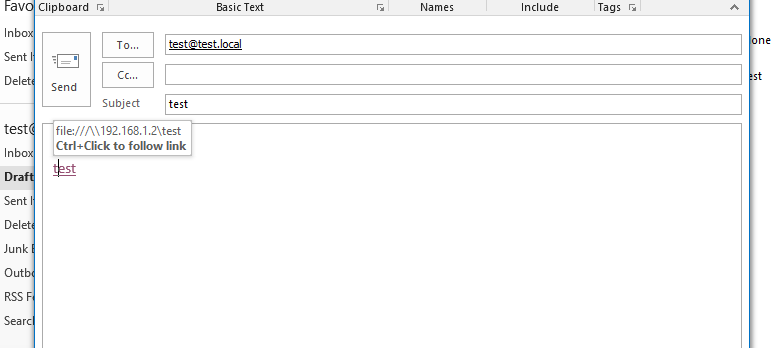
(Thường thì windows sẽ có tự động chặn ICMP)

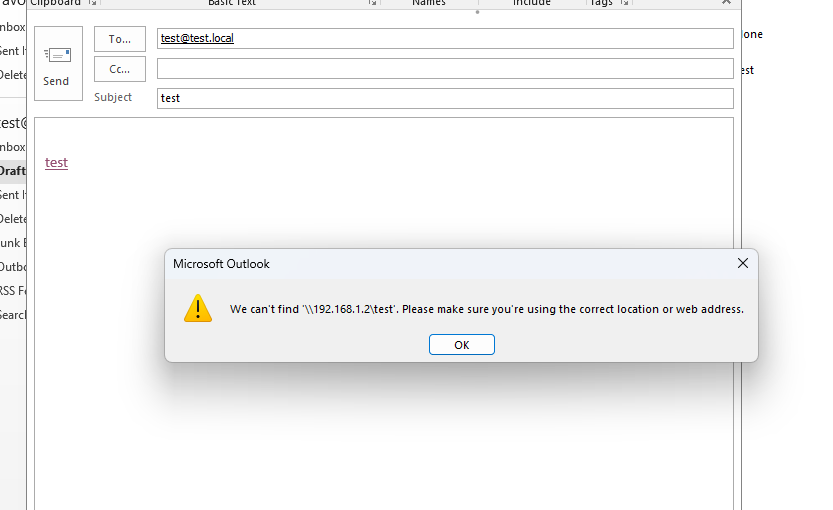
* Tới đây là các bạn đã xong phần chuẩn bị. Chúng ta bắt đầu thôi.

**2 Triển Khai Tấn Công**

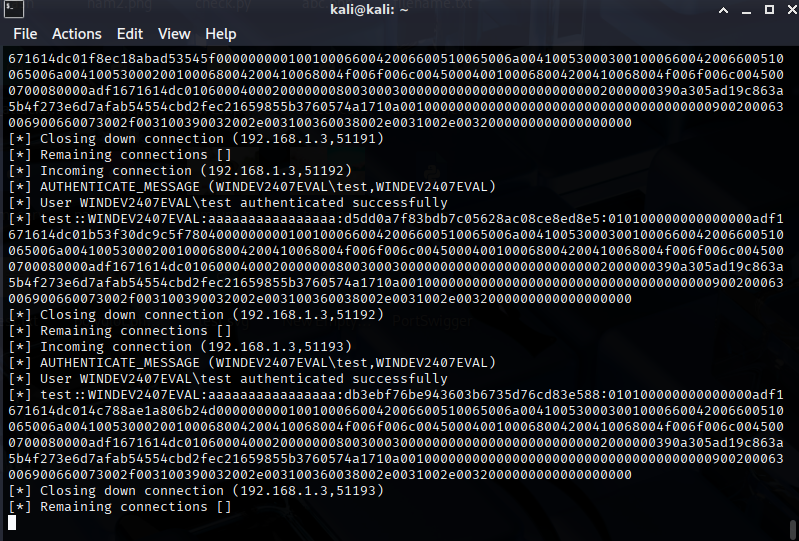
1. **Bật impacket smb server***(attacker)*sudo python3 /usr/share/doc/python3-impacket/examples/smbserver.py test /tmp/test -smb2support



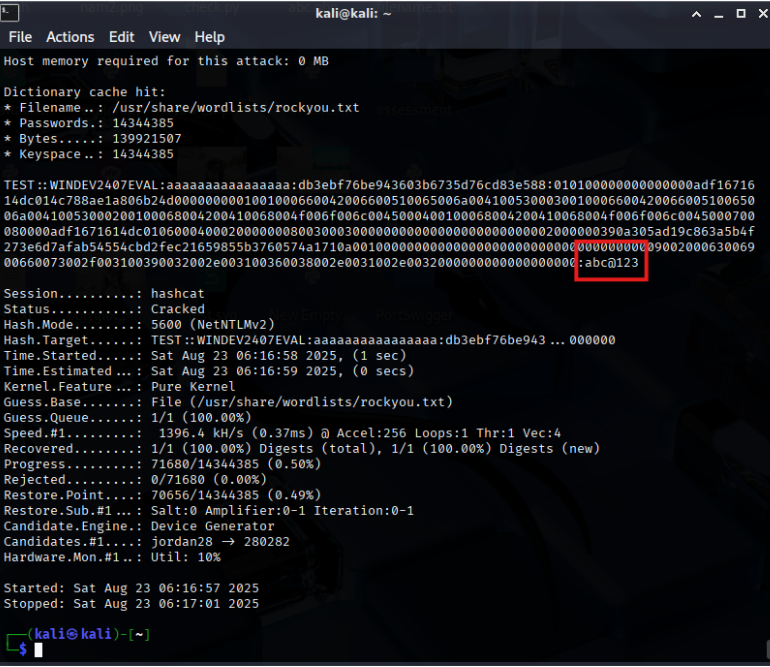
1. **Gửi email cho target  
   ***(mô phỏng bằng cách viết trên để trên drafts cũng được vẫn cùng một hình thức)*
2. **Xuất hiện lỗ hổng**Khi victim nhấn vào link UNC attacker có thể bắt được NTLMv2 hash

****

*(hình ảnh khi victim nhấn vào link UNC)*



*(hình ảnh attacker lấy được NTLMv2 hash)*

1. **Burp force NTLMv2**Sử dụng công cụ hashcat để đoán password. Trước khi đó để có cái nhìn tổng quan chúng ta lưu NTLMv2 hash vào 1 file txt để dễ kiểm soát rồi sau đó sử dụng lệnh: hashcat -m 5600 hash.txt /usr/share/wordlists/rockyou.txt –force  
   **  
   *(hình ảnh sau khi burp thành công)*

***Vậy bây giờ chúng ta có user:test password:abc@123 Thành Công!***

**Kết luận Lab – CVE‑2023‑23397: Outlook NTLM Relay / RCE**

1. **Mục tiêu lab**

* Mô phỏng tấn công Outlook RCE thông qua NTLM relay.
* Thực hành capture NTLMv2 hash từ user Outlook khi click UNC link độc hại.
* Thể hiện cơ chế Remote Code Execution (RCE) dựa trên relay NTLM.

1. **Các bước thực hiện**

* **Chuẩn bị môi trường lab:** *(mới đầu mình chạy bằng responder nhưng nhận ra nếu gán link UNC để ẩn ip attacker thì popup lên nhập tài khỏa tức là hong tự động được nên mình chuyển sang impacket SMB server để triển khai auto aut cho chuyên nghiệp hehe)*
  + Kali Linux (attacker) → chạy Responder hoặc Impacket SMB server để capture hash.
  + Windows 10/11 VM (victim) → Outlook 2016/2019/2021.
* **Gán UNC link độc hại vào body mail Outlook.**
* **Khi victim click link:**
  + Windows tự gửi NTLMv2 hash tới SMB server trên Kali.
  + Không cần nhập password thủ công (hash tự động gửi).
* Hash đã capture → có thể crack offline bằng hashcat hoặc dùng trực tiếp để Pass-the-Hash.

1. **Kết quả lab**

* **Lab thành công khi:**
  + Kali log nhận được NTLMv2 hash từ Windows/Outlook.
  + Có thể dùng hash để đăng nhập SMB hoặc RDP.
  + Đã chứng minh được nguy cơ RCE/credential relay qua Outlook.

1. **Bài học rút ra**

* Outlook tự động gửi hash NTLM qua UNC/SMB nếu click link → tiềm ẩn rủi ro cao.
* NTLM relay attack có thể dùng để leo privilege hoặc lấy credentials offline.
* Việc cấu hình SMB/NTLM hardening và Outlook security là cần thiết để giảm rủi ro.
* Lab cũng minh họa tính hiệu quả của PoC trong môi trường isolated, cho phép đánh giá lỗ hổng mà không gây nguy hiểm cho môi trường thật.

1. **Kết luận tổng quan**

* CVE‑2023‑23397 là một lỗ hổng nghiêm trọng liên quan tới Outlook & NTLM relay.
* Lab cho thấy kỹ thuật tấn công có thể capture hash và leo privilege trong mạng LAN.
* Đây là ví dụ điển hình về việc tấn công mạng nội bộ thông qua giao thức xác thực cũ (NTLM) và nhấn mạnh tầm quan trọng của việc patch, bảo mật SMB/Outlook, cũng như awareness của user.