BÁO CÁO BÀI THỰC HÀNH SỐ 7

**PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG**

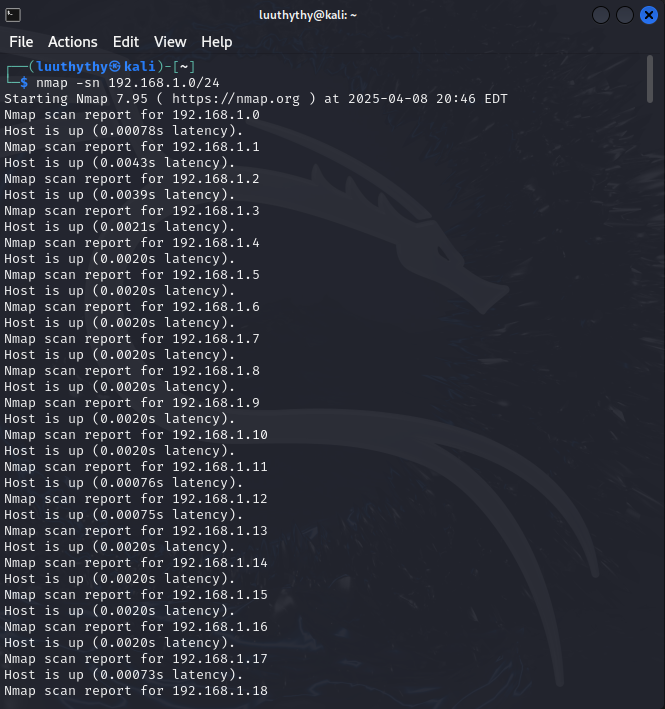
Họ và tên sinh viên: Lưu Thy Thy

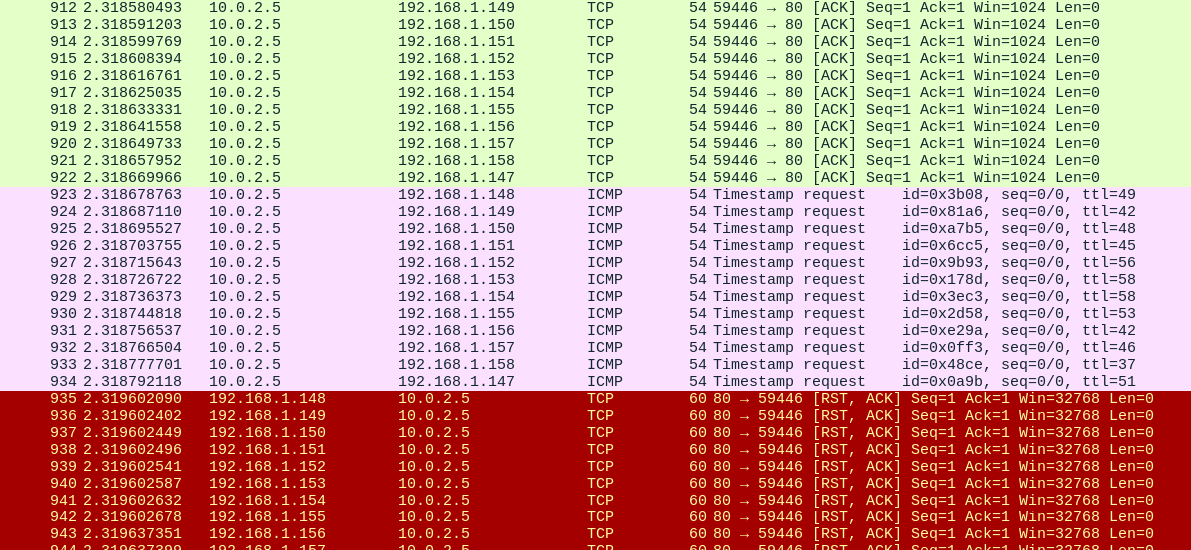
MSSV: 1050080078

**KẾT QUẢ THỰC HÀNH**

1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**
   1. **Kịch bản 1**

Thực hiện lệnh quét nmap –sn Dia\_chi\_mang/Mat\_na trên máy do thám. Dựa trên việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì? Lưu lại file lưu lượng trên máy do thám với tên là task1.pcap.





**Phân tích lưu lượng:**



Gói 611 – TCP [ACK]

* Nguồn: 10.0.2.5
* Đích: 192.168.1.78
* Port: 59446 → 80
* Cờ: ACK
* Chi tiết: Gửi gói TCP có cờ ACK mà không có kết nối trước đó (không phải phần của một phiên TCP hợp lệ).
* Ý nghĩa: Gói ACK này có thể là một phần của TCP ACK Scan hoặc TCP Idle Scan, dùng để kiểm tra phản hồi từ cổng đích mà không thiết lập kết nối hoàn chỉnh.



Gói 623 – ICMP Timestamp request

* Loại: ICMP (Internet Control Message Protocol)
* Thông điệp: Timestamp request
* TTL: 45
* Ý nghĩa: Đây là kỹ thuật thu thập thông tin hệ thống bằng cách yêu cầu thời gian hiện tại từ thiết bị đích. Mục tiêu là: Kiểm tra sự hiện diện của máy chủ và phát hiện hệ điều hành thông qua định dạng phản hồi thời gian.



Gói 635 – TCP [RST, ACK]

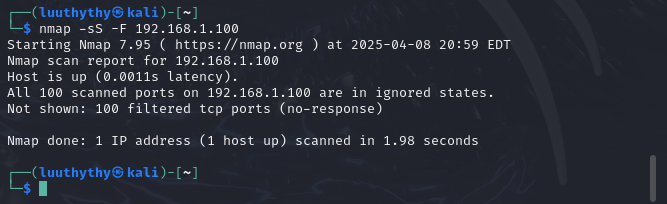
* Nguồn: 192.168.1.78 (máy bị quét)
* Đích: 10.0.2.5
* Port: 80 → 59446
* Cờ: RST, ACK
* Ý nghĩa: Máy đích gửi lại gói RST, ACK, báo hiệu rằng không có phiên kết nối hợp lệ tồn tại với gói ACK trước đó. Đây là phản ứng điển hình khi một TCP ACK Scan được thực hiện.

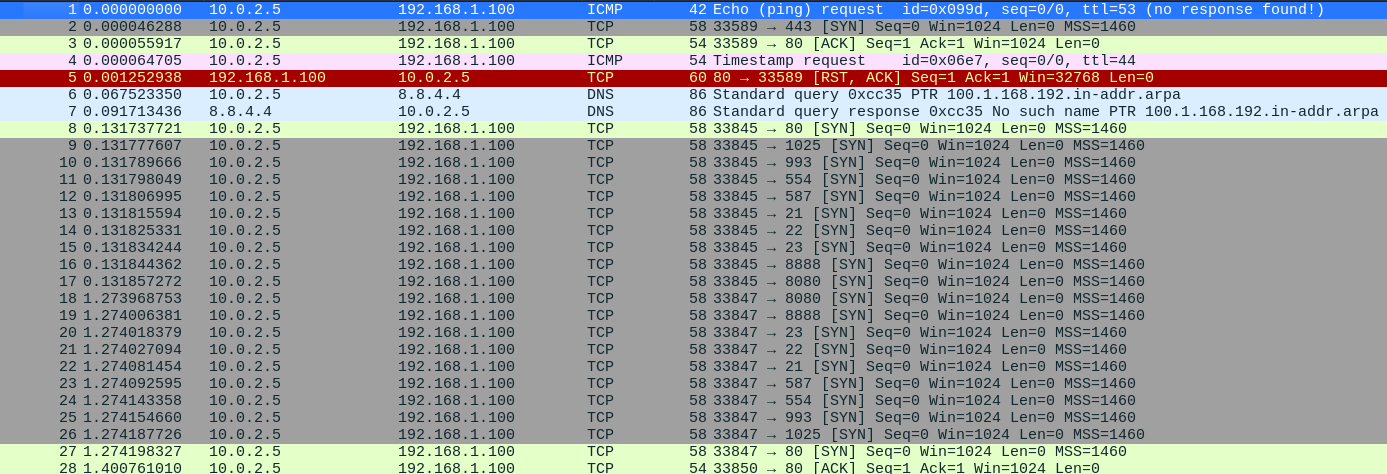
**Kết luận: Kỹ thuật quét thăm dò là gì?**

Kỹ thuật quét được sử dụng ở đây là:

* TCP ACK Scan: Gửi gói ACK đến cổng đích để xác định xem firewall có lọc cổng hay không.
  + Nếu nhận lại RST → cổng không bị lọc.
  + Nếu không có phản hồi → có thể bị lọc bởi firewall.
* ICMP Timestamp Request: Thu thập thông tin thời gian hệ thống → dùng cho OS fingerprinting hoặc kiểm tra độ trễ mạng.
  1. **Kịch bản 2**

Thực hiện lệnh quét nmap –sS –F Địa\_chỉ\_IP\_máy\_mục\_tiêu trên máy do thám. Dựa trên việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì? Lưu lại file lưu lượng trên máy do thám với tên là task2.pcap.





**Phân tích lưu lượng:**



Gói 2 – TCP [SYN] đến port 443

* 10.0.2.5 → 192.168.1.100, gửi gói TCP SYN đến cổng 443 (HTTPS).
* Đây là gói đầu tiên trong tiến trình bắt tay 3 bước (TCP 3-way handshake).



Gói 3 – TCP [ACK] đến port 80

* Gửi TCP ACK đến cổng 80, không có kết nối trước đó.
* Đây là điểm bất thường, vì thường phải có SYN trước đó mới có ACK.
* Cho thấy dấu hiệu của một ACK Scan.



Gói 4 – ICMP Timestamp Request

* Gửi yêu cầu ICMP Timestamp → dùng để thu thập thông tin hệ thống từ máy đích.



Gói 5 – TCP [RST, ACK] từ port 80

* Máy đích phản hồi lại bằng RST, ACK → xác nhận rằng không có kết nối hợp lệ.
* Đây là phản ứng điển hình cho ACK Scan



Gói 6–7 – DNS PTR Query

* Thực hiện truy vấn DNS ngược (Reverse DNS Lookup) với IP đích 192.168.1.100 để lấy tên miền.
* Mục đích: Thu thập thông tin về tên máy chủ đích.



Gói 28 – TCP [ACK] khác đến port 80

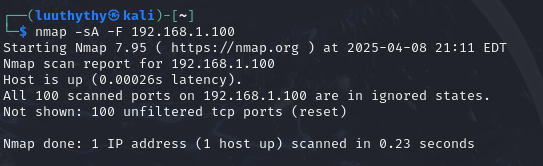
* Một lần nữa gửi ACK đến port 80 từ một cổng nguồn khác (33850) → có vẻ là lặp lại kỹ thuật ACK scan từ cổng khác để kiểm tra phản ứng.

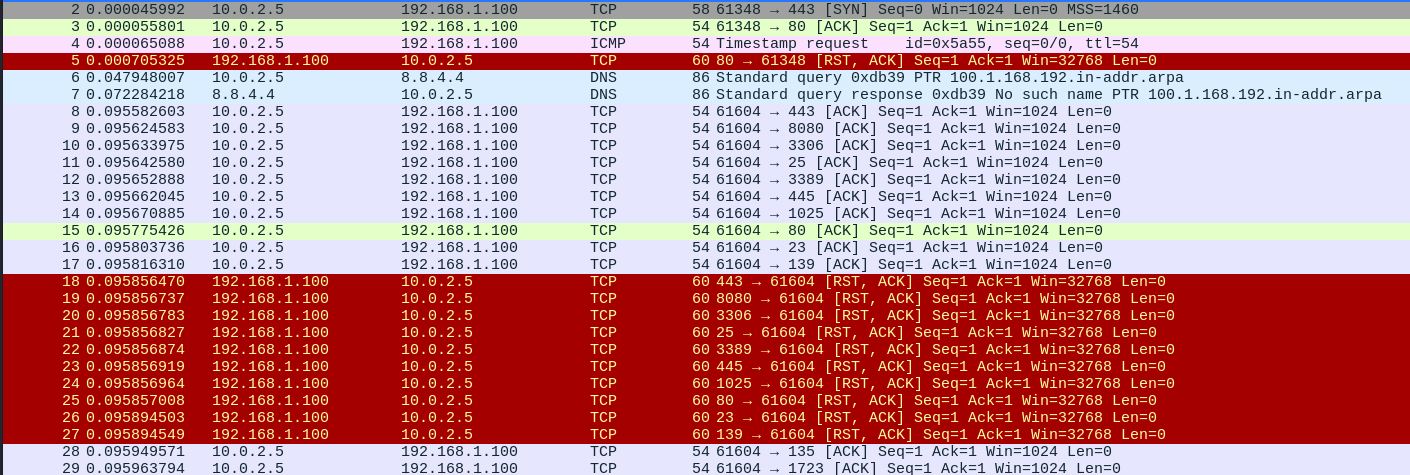
**Kỹ thuật quét được sử dụng**

Dựa trên các dấu hiệu trên, ta có thể xác định kỹ thuật quét được sử dụng là:

* TCP ACK Scan
  + Dấu hiệu: Gửi gói TCP có cờ ACK đến cổng đích mà không có kết nối trước đó
  + Mục tiêu: Xác định xem cổng có bị tường lửa lọc hay không.
  + Nếu nhận được RST → cổng mở hoặc không bị lọc
  + Nếu không có phản hồi → cổng có thể bị lọc bởi firewall
  + Gói liên quan: Gói 3 và Gói 28 (ACK), gói 5 (RST, ACK).
* TCP SYN Scan
  + Gói 2 là một gói SYN đến port 443 – dấu hiệu của SYN scan.
  + Đây là kỹ thuật phổ biến nhất để quét cổng:
    - Nếu nhận SYN-ACK → cổng mở.
    - Nếu nhận RST → cổng đóng.
* ICMP Timestamp Request
  + Sử dụng ICMP để thu thập thông tin hệ điều hành hoặc kiểm tra độ trễ thời gian hệ thống.
* ICMP Timestamp Request
  + Sử dụng ICMP để thu thập thông tin hệ điều hành hoặc kiểm tra độ trễ thời gian hệ thống.
  1. **Kịch bản 3**

Thực hiện lệnh quét nmap –sA –F Địa\_chỉ\_IP\_máy\_mục\_tiêu trên máy do thám. Dựa trên việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì? Lưu lại file lưu lượng trên máy do thám với tên là task3.pcap.





Phân tích lưu lượng



Gói 3 – TCP [ACK] đến cổng 80

* 10.0.2.5 → 192.168.1.100, gửi gói ACK đến port 80, nhưng không có gói SYN trước đó.
* Đây không phải một phiên TCP hợp lệ → dấu hiệu của ACK Scan.



Gói 4 – ICMP Timestamp Request

* Gửi gói ICMP yêu cầu thời gian hệ thống → mục tiêu: thu thập thông tin hệ điều hành hoặc độ trễ mạng.



Gói 5 – TCP [RST, ACK] từ 192.168.1.100

* Phản hồi từ máy đích cho biết không có phiên TCP hợp lệ.
* Đây là kết quả mong đợi trong ACK Scan: nếu nhận RST thì cổng không bị lọc.



Gói 6–7 – DNS truy vấn PTR

* Gửi yêu cầu truy vấn DNS ngược (PTR) cho IP đích (192.168.1.100), qua DNS server 8.8.4.4.
* Thu thập hostname từ địa chỉ IP (Reconnaissance).





Gói 8 – TCP [ACK] đến port 443 và Gói 15 – TCP [ACK] đến port 80 (khác cổng nguồn)

* Tiếp tục gửi ACK đến các cổng khác nhau (443, 80) từ cổng nguồn khác (61604).
* Lặp lại kiểu ACK Scan để kiểm tra nhiều cổng.



Gói 18 – TCP [RST, ACK] từ port 443

* Phản hồi RST, ACK từ port 443 → xác nhận tiếp tục là phản hồi của ACK Scan.

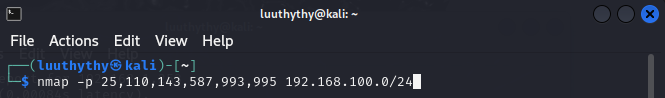
**Kết luận**

Kỹ thuật quét sử dụng trong phiên này bao gồm:

* TCP ACK Scan => Mục tiêu: Kiểm tra chính sách tường lửa (firewall rules) trên các cổng như 80, 443.
* ICMP Timestamp Request => Mục tiêu: Thu thập thông tin hệ thống, hỗ trợ fingerprinting.
* DNS Reverse Lookup (PTR) => Mục tiêu: Thu thập thông tin hostname từ IP đích.

1. **Thu thập thông tin hệ thống**

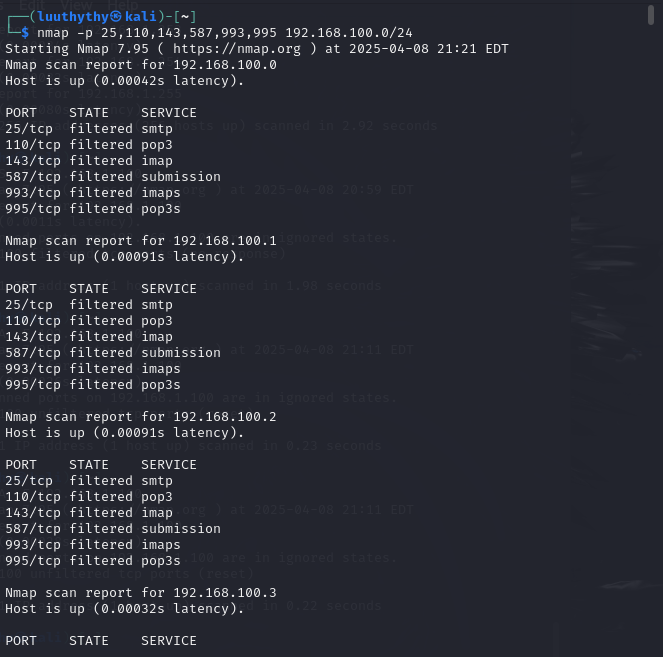
Hãy cho biết lệnh quét thăm dò tìm kiếm máy chủ email là gì? Giải thích các tham số sử dụng trong lệnh này?(1 điểm)

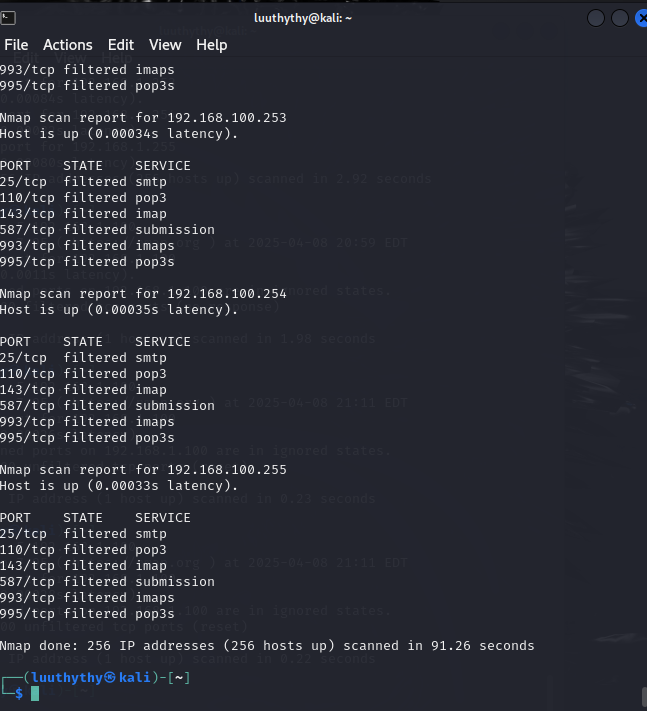


* nmap: Là công cụ quét mạng mã nguồn mở, dùng để phát hiện host, dịch vụ, cổng mở, phiên bản ứng dụng, và hệ điều hành trên mạng.
* -p 25,110,143,587,993,995:
  + -p: Tùy chọn chỉ định cổng cần quét.
* Danh sách cổng:
  + 25: SMTP (Simple Mail Transfer Protocol) – Gửi email.
  + 110: POP3 (Post Office Protocol v3) – Nhận email (không mã hóa).
  + 143: IMAP (Internet Message Access Protocol) – Quản lý email từ xa (không mã hóa).
  + 587: Submission (SMTP over TLS/SSL) – Gửi email an toàn.
  + 993: IMAPS (IMAP over SSL/TLS) – Quản lý email an toàn.
  + 995: POP3S (POP3 over SSL/TLS) – Nhận email an toàn.
* Mục đích: Quét các cổng liên quan đến dịch vụ email để kiểm tra trạng thái hoặc bảo mật.
* 192.168.100.0/24:
  + Địa chỉ mạng: Chỉ định dải IP từ 192.168.100.0 đến 192.168.100.255 (256 host).
  + /24: Subnet mask 255.255.255.0 – Mạng lớp C.
  + Mục đích: Quét toàn bộ mạng con 192.168.100.x.

Thông tin hệ điều hành:

- Hình ảnh chụp kết quả của nmap: 0.25 điểm



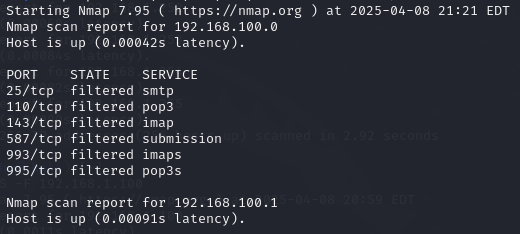


- Nêu tên và phiên bản hệ điều hành: 0.25 điểm

* Không xác định được qua kết quả scan này.
* Lý do: Các cổng đều ở trạng thái filtered, Nmap không thu thập đủ dữ liệu để phân tích OS fingerprinting.

Thông tin dịch vụ: 1 điểm

- Hình ảnh chụp kết quả của nmap: 0.25 điểm



Kết quả scan hiển thị tất cả cổng 25, 110, 143, 587, 993, 995 đều có trạng thái filtered

- Danh sách dịch vụ: 0.75 điểm

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
| 1 | SMTP | 25/tcp | Không xác định (filtered) |
| 2 | POP3 | 110/tcp | Không xác định (filtered) |
| 3 | IMAP | 143/tcp | Không xác định (filtered) |
| 4 | Submission (SMTP) | 143/tcp | Không xác định (filtered) |
| 5 | IMAPS | 993/tcp | Không xác định (filtered) |
| 6 | POP3S | 995/tcp | Không xác định (filtered) |

* Khi cổng bị filtered, việc phát hiện OS/dịch vụ bằng Nmap gần như không khả thi.

1. **Tìm kiếm thông tin về các lỗ hổng**

Báo cáo ngắn gọn về các lỗ hổng đã được công bố trên các phần mềm cung cấp dịch vụ.

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ (tên dịch vụ, tên phần mềm, phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng (Tiếng Việt)** |
| Microsoft Windows MSHTML Platform | CVE-2024-30040 | Lỗ hổng cho phép kẻ tấn công vượt qua cơ chế bảo vệ, khai thác từ xa qua lỗ hổng trong xử lý HTML. |
| Microsoft Windows DWM Core | CVE-2024-30051 | Lỗ hổng leo thang đặc quyền thông qua thư viện DWM Core, cho phép chiếm quyền điều khiển hệ thống. |
| Microsoft SharePoint Server | CVE-2024-30044 | Lỗ hổng thực thi mã từ xa, cho phép kẻ tấn công chèn mã độc qua các yêu cầu không an toàn. |
| Gladinet CentreStack | CVE-2025-30406 | Sử dụng khóa mã hóa cứng, cho phép kẻ tấn công thực thi mã từ xa qua payload giả mạo. |
| Microsoft Windows CLFS Driver | CVE-2025-29824 | Lỗ hổng "use-after-free" trong driver CLFS, cho phép leo thang đặc quyền cục bộ. |
| CrushFTP | CVE-2025-31161 | Lỗ hổng bypass xác thực, cho phép kẻ tấn công đăng nhập vào tài khoản bất kỳ (ví dụ: crushadmin). |
| Fortinet FortiOS/FortiProxy | CVE-2025-24472 | Lỗ hổng bypass xác thực, cho phép truy cập trái phép vào hệ thống mạng. |