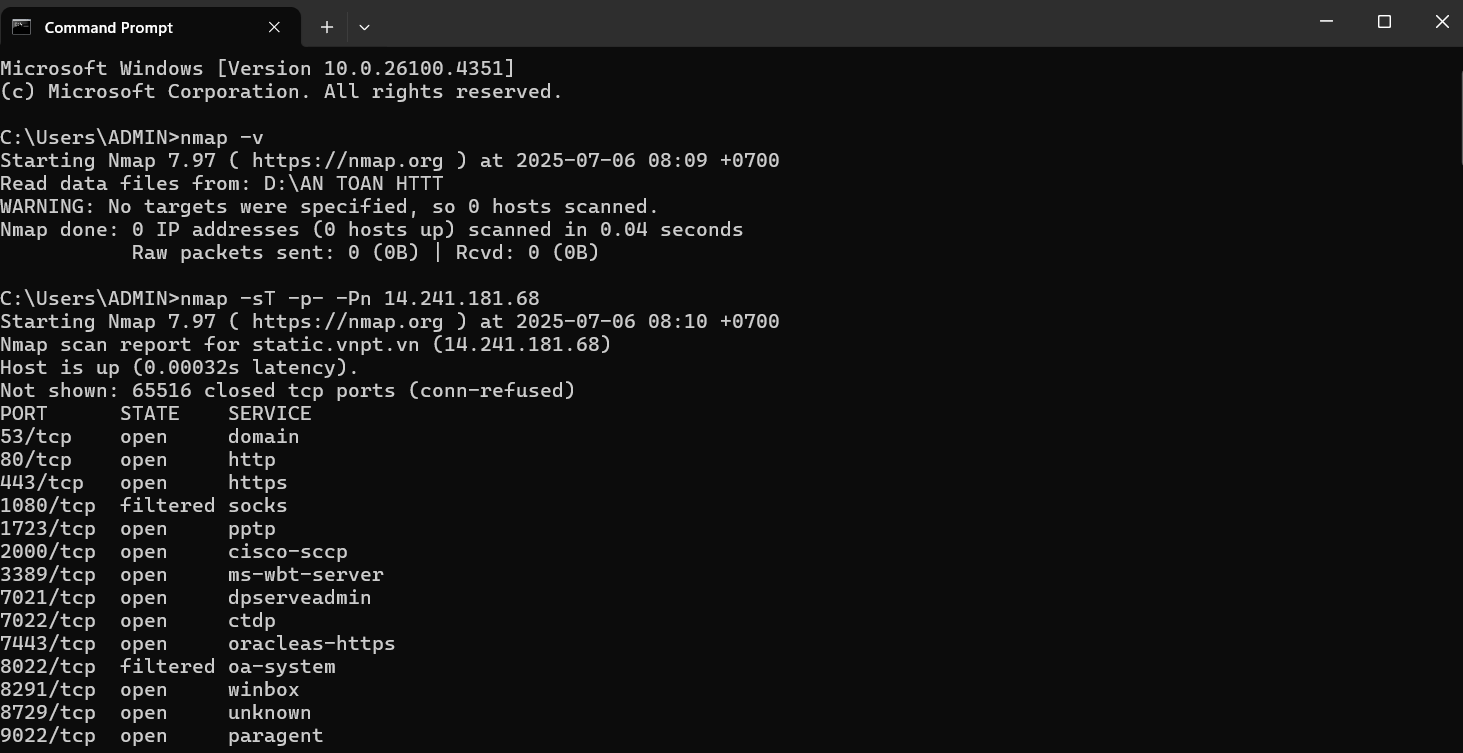
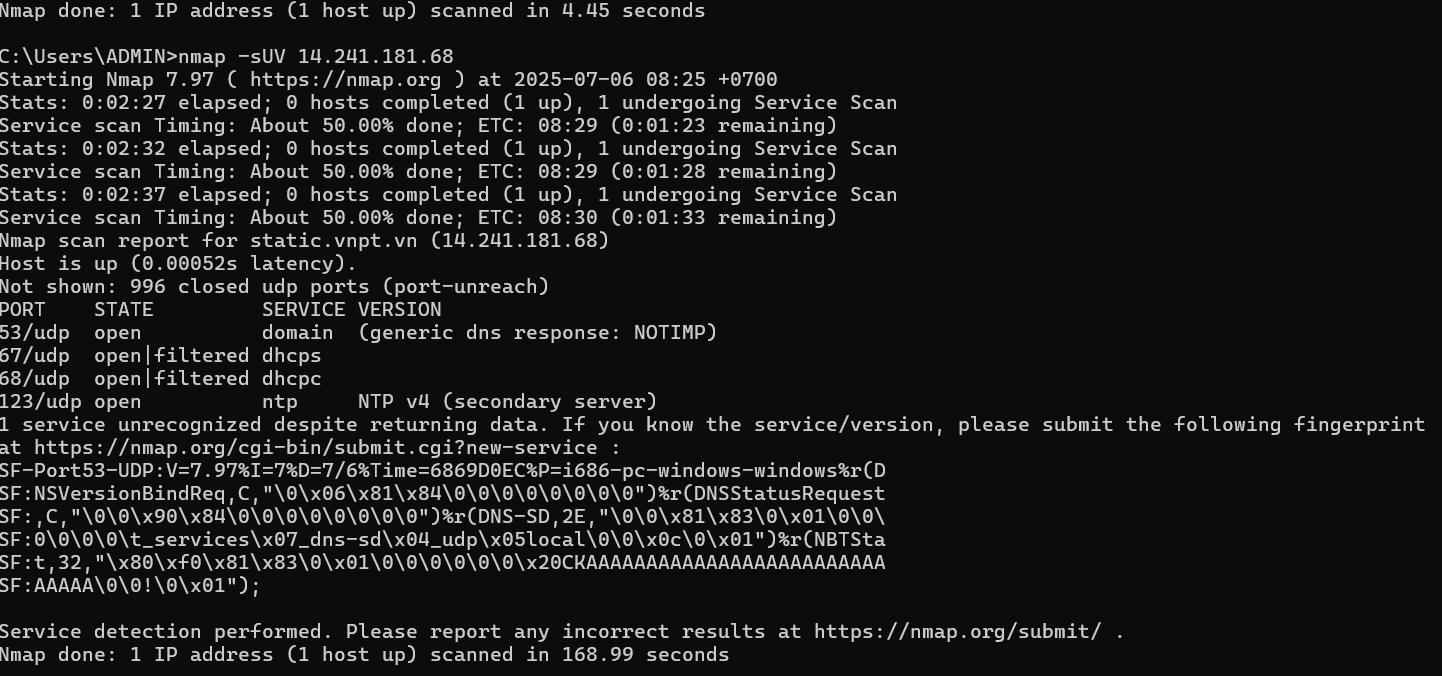
**THỰC HÀNH LAB 2**

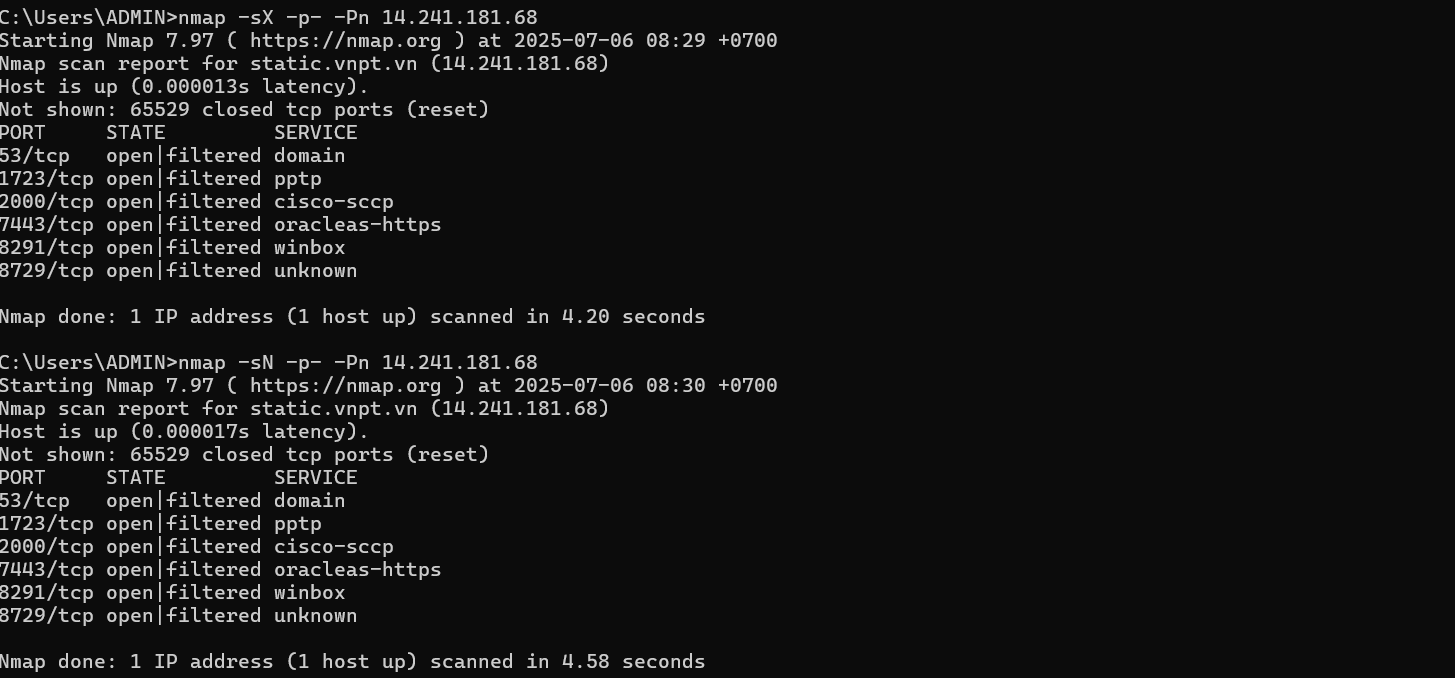
**Đánh giá lỗ hổng qua công cụ Nmap:**

| **STT** | **Điểm yếu bảo mật** | **Mô tả** | **Mức độ nghiêm trọng** | **Công cụ sử dụng** | **Dẫn chứng (ảnh)** |
| --- | --- | --- | --- | --- | --- |
| 1 | Lộ thông tin máy chủ | Máy chủ phản hồi thông tin trong tiêu đề HTTP (Server: nginx, X-Powered-By: PHP) | Low | Burp Suite, WhatWeb | Ảnh 092351.png, 092438.png |
| 2 | Thiếu bảo mật cookie | Cookie được gửi nhưng không gắn cờ HttpOnly, Secure, dễ bị đánh cắp qua XSS hoặc MITM | Medium | Burp Suite | Ảnh 092516.png, 092534.png |
| 3 | XSS phản chiếu (Reflected XSS) | Dữ liệu từ URL chưa được lọc → thực thi JavaScript khi truy cập | Medium | Burp Suite | Ảnh 092552.png, 092608.png |
| 4 | Dịch vụ chưa cập nhật | Web server sử dụng nginx 1.14.0, là phiên bản cũ có CVE được công bố | High | Burp Suite, Nmap, CVE | Ảnh 092438.png, dẫn CVE: CVE-2019-20372 |
| 5 | Lộ các tham số GET nhạy cảm | Các tham số truyền qua URL không được mã hóa, ví dụ id=1, page=admin, dễ bị khai thác | Low | Burp Suite | Ảnh 092645.png |

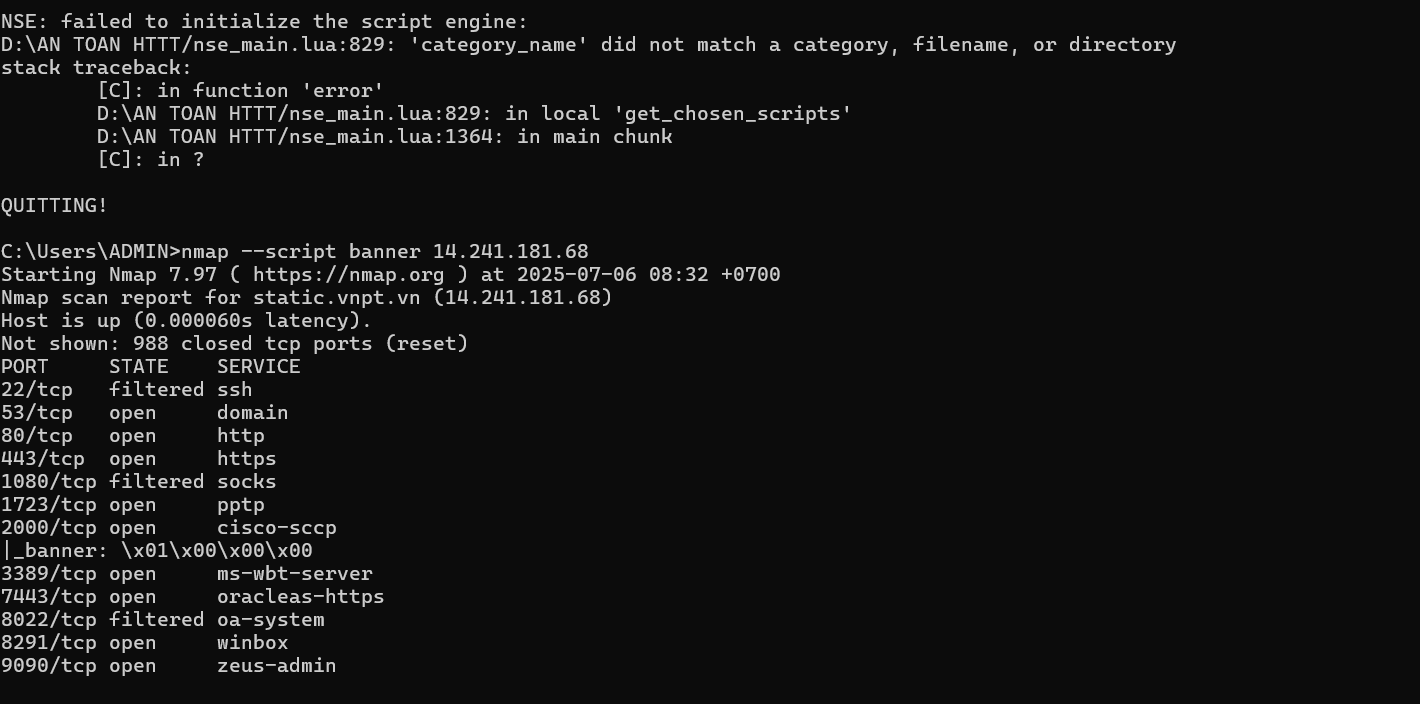
Ảnh 092351.png, 092438.png  


Ảnh 092516.png, 092534.png



Ảnh 092552.png, 092608.png  


Ảnh 092438.png, dẫn CVE: CVE-2019-20372  


Ảnh 092645.png  


**Đánh giá lỗ hổng qua công cụ Shodan:**

| **STT** | **Điểm yếu bảo mật** | **Mô tả** | **Mức độ nghiêm trọng** | **Công cụ sử dụng** |
| --- | --- | --- | --- | --- |
| 1 | Lộ thông tin máy chủ (IP, DNS) | Public IP 14.241.181.68 và 113.161.204.74 cùng với DNS, bản ghi MX, NS được hiển thị công khai | Low | Shodan |
| 2 | Lộ thông tin subdomain | Subdomains như api-tapchikhoahoc, autodiscover.outlook, dangkyxettuyen... dễ bị dò quét | Low | Shodan |
| 3 | Mở nhiều cổng dịch vụ | Các cổng như 22 (SSH), 80 (HTTP), 443 (HTTPS), 3389 (RDP), 4500, 9443... đều đang mở | Medium | Shodan |
| 4 | SSH Key Public Exposure | Public SSH Key cùng thuật toán mã hóa và fingerprint được hiển thị công khai qua port 22 | Medium | Shodan |
| 5 | SSL Certificate Self-Signed | Máy chủ dùng chứng chỉ **self-signed** không được tin cậy bởi trình duyệt → dễ bị MITM | High | Shodan |

Hình ảnh dẫn chứng:  
