**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**CƠ SỞ TẠI THÀNH PHỐ HỒ CHÍ MINH**



**BÀI TẬP 2:**

***Report NMAP SCRIPTS***

**Môn :** Kiểm Thử Xâm Nhập

Giảng viên: Huỳnh Thanh Tâm

Nhóm 21: Chế Công Hậu – N17DCAT023

Nguyễn Thịnh Phát – N17DCAT053

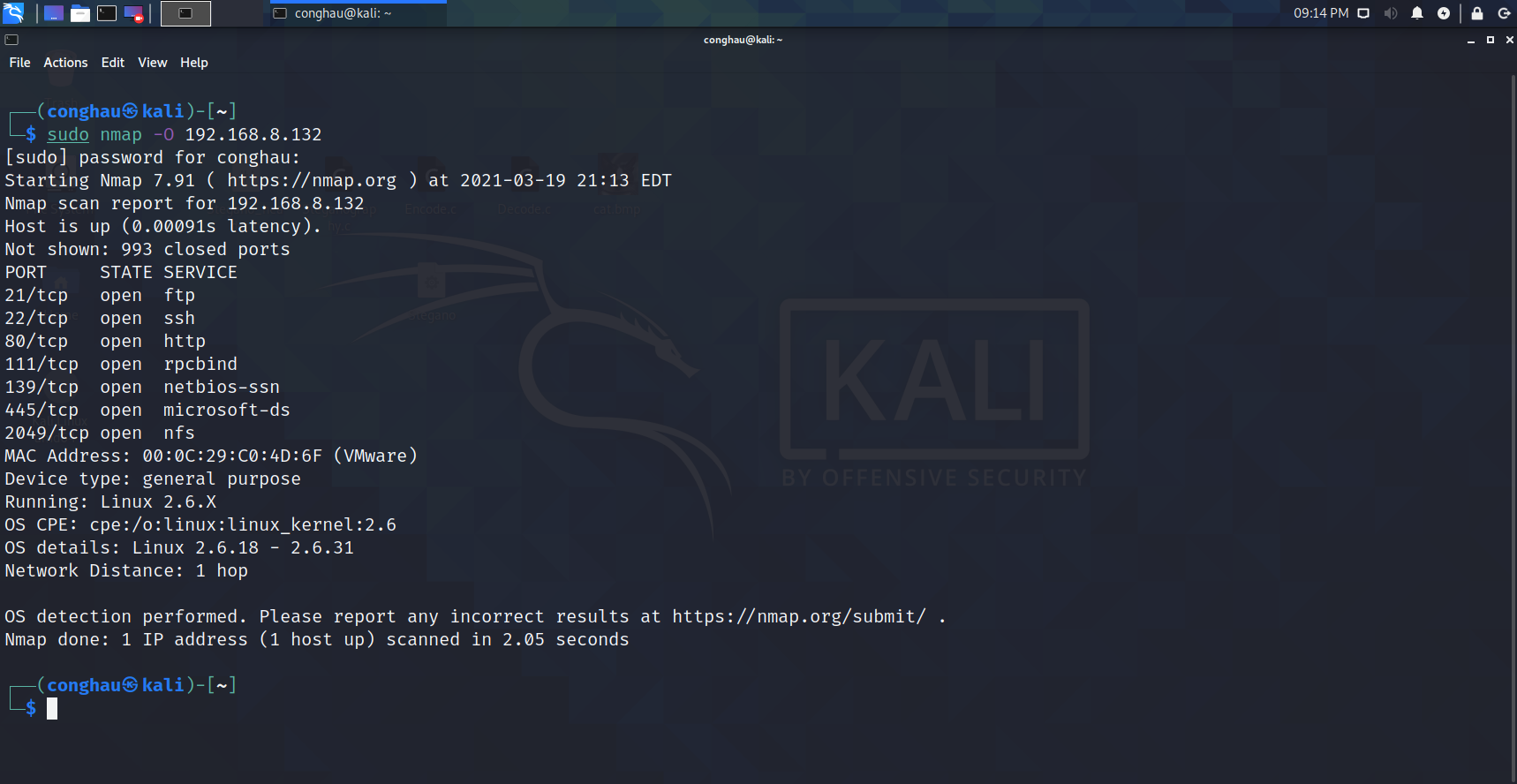
Trần Huỳnh Hoàng My – N17DCAT046

*Ngày 20 tháng 3 năm 2021*

Thực hiện scan Web Server Book Ubuntu ( có địa chỉ IP là **192.168.8.132**) bằng tool NMAP.

Scan sơ bộ hệ thống và port của Book Ubuntu bằng câu lệnh sau:

**sudo nmap -O 192.168.8.132**



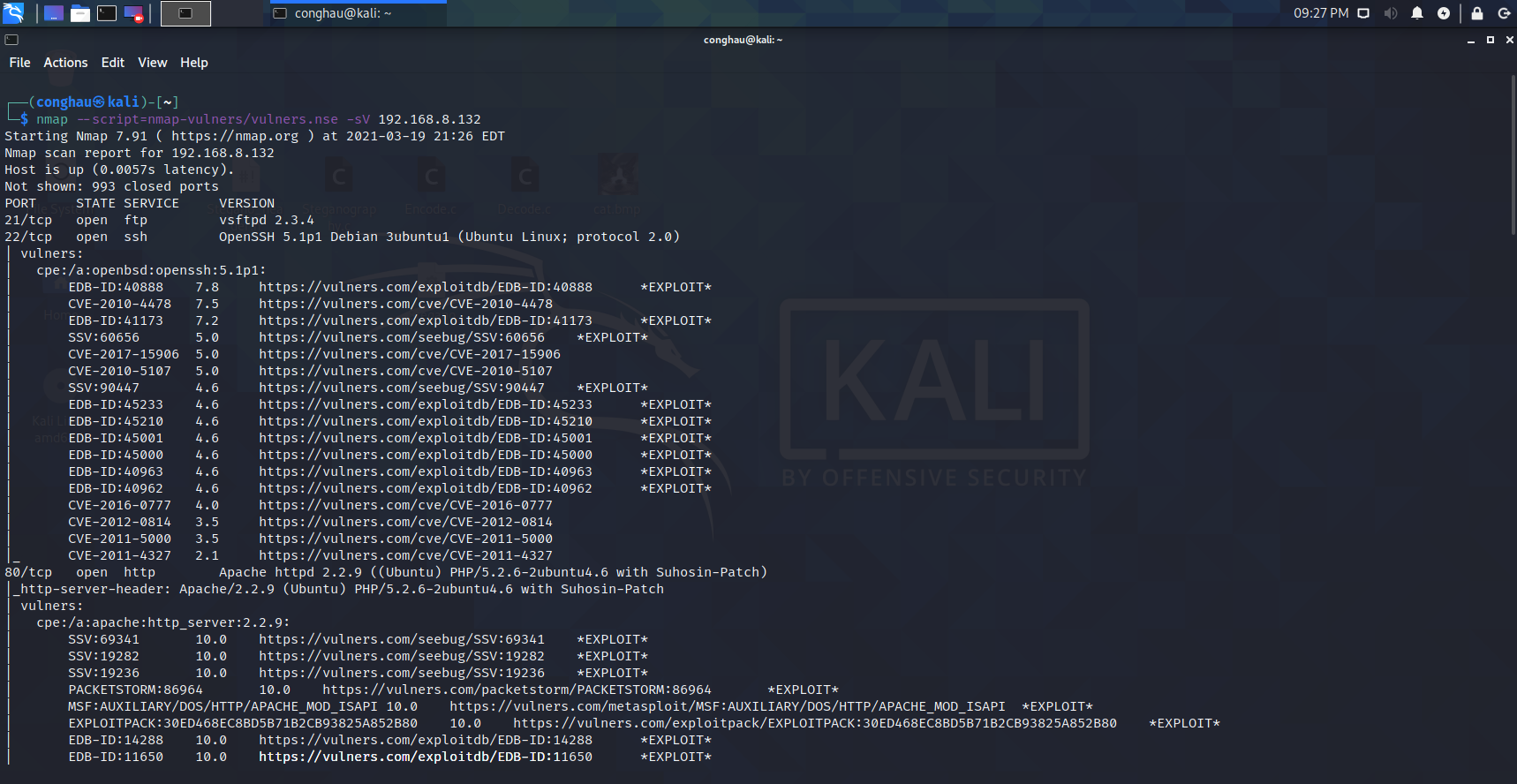
Dựa vào nmap, ta có thể thấy được rằng Book Ubuntu đang chạy hệ điều hành Linux kernel 2.6. Có các service đang chạy như hình trên: ftp, ssh, http, …

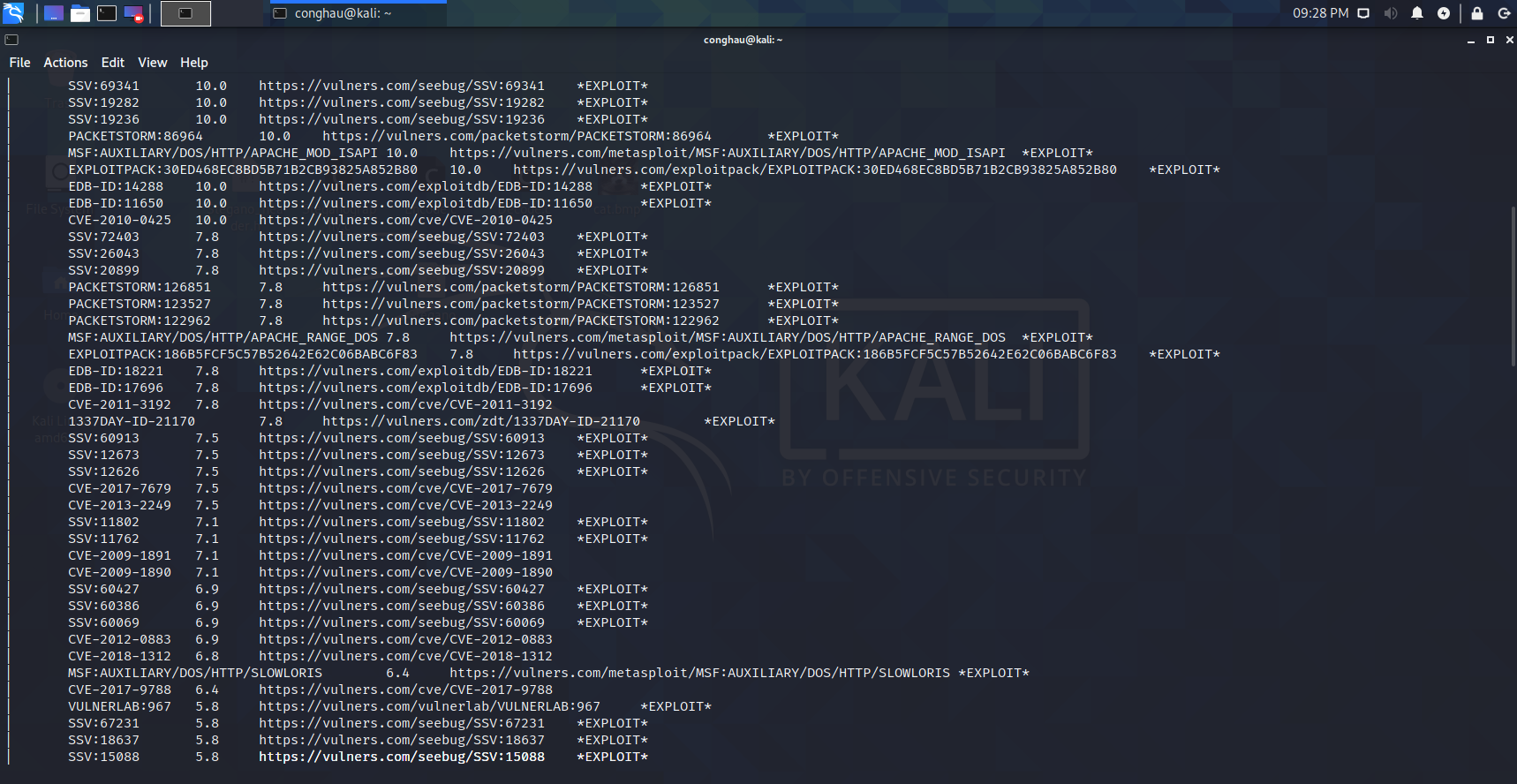
Sử dụng script vulners.nse của nmap-vulners

Cách cài đặt script vulners:

* cd /usr/share/nmap/scripts
* git clone <https://github.com/vulnersCom/nmap-vulners.git>
* sudo nmap --script-updatedb

Scan bằng lệnh: **nmap --script=nmap-vulners/vulners.nse -sV 192.168.8.132**





Danh sách một số các lỗ hổng được tìm thấy bằng scrip vulners:

|  |  |  |
| --- | --- | --- |
| TÊN CVE | MÔ TẢ | CÁCH PHÁT HIỆN |
| CVE-2017-15906 | * **Type** cve * **Reporter** [cve@mitre.org](mailto:cve@mitre.org) * **Modified** 2020-08-24 17:37:00   Điểm yếu liên quan đến dịch vụ **SSH**.  Hàm process\_open trong sftp-server.c trong OpenSSH phiên bản trước 7.6 không ngăn chặn được hoàn toàn các hoạt động ghi ở chế độ read-only, cho phép kẻ tấn công tạo các tệp có độ dài bằng không.  **Tài liệu tham khảo:**  <https://vulners.com/cve/CVE-2017-15906>  **CVSS**: 5.0 | Scan bằng script vulners của công cụ nmap-vulners. |
| CVE-2018-1312 | * **Type** cve * **Reporter** [cve@mitre.org](mailto:cve@mitre.org) * **Modified** 2019-07-29 19:15:00   Điểm yếu liên quan đến dịch vụ **HTTP**.  Trong Apache httpd 2.2.0 đến 2.4.29, khi tạo xác thực HTTP Digest, Nonce được gửi để ngăn các cuộc tấn công reply không được tạo ra hoàn toàn bằng cách sử dụng seed giả một cách ngẫu nhiên. Trong một cụm máy chủ sử dụng cấu hình xác thực Digest, kẻ tấn công có thể phát lại các HTTP Requests trên các máy chủ mà không bị phát hiện.  **Tài liệu tham khảo:** <https://vulners.com/cve/CVE-2018-1312>  **CVSS**: 6.8 | Scan bằng script vulners của công cụ nmap-vulners. |
| CVE-2017-7679 | * **Type** cve * **Reporter** [cve@mitre.org](mailto:cve@mitre.org) * **Modified** 2020-04-01 15:15:00   Điểm yếu liên quan đến dịch vụ **HTTP**.  Trong các phiên bản Apache httpd 2.2.x trước phiên bản 2.2.33 và các phiên bản 2.4.x trước phiên bản 2.4.26, mod\_mime có thể đọc được một byte thông qua phần cuối của bộ đệm khi gửi các header phản hồi loại Content-Type độc hại.  **Tài liệu tham khảo:** <https://vulners.com/cve/CVE-2017-7679>  **CVSS**: 7.5 | Scan bằng script vulners của công cụ nmap-vulners. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |