Nguyễn Bá Hùng\_CNPM3\_1050080264

Bước 1: vào terminal trong Kali gõ Wireshark

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Sau đó mở terminal mới gõ

Nmap -sn 192.168.117.0/24

A screenshot of a computer

AI-generated content may be incorrect.

Có thể thấy ngoài địa chỉ 192.168.117.10 là địa chỉ của máy tấn công thì còn 3 nút mạng nữa đang hoạt động có địa chỉ là 192.168.117.2, 192.168.117.3 và 192.168.117.13

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

- Nhập giá trị tcp vào bộ lọc. Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy gói tin TCP SYN/ACK được gửi từ cổng 23 từ địa chỉ 192.168.117.13 về máy tấn công. Như vậy, điều này là phù hợp với kết quả của Nmap đã trả về (Địa chỉ 192.168.117.10 trong kết quả trả về là địa chỉ của chính máy tấn công vì máy này cũng cung cấp dịch vụ Telnet)

Bước 1: Truy cập máy ảo Attack Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin. Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau: nmap -sT 192.168.117.13 Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có kết quả tương tự như dưới đây. Kết quả cho thấy các cổng dịch vụ 22, 23, 53 trên máy mục tiêu 192.168.117.13 có trạng thái open. Ta có thể phán đoán máy này đang cung cấp các dịch vụ tương ứng là ssh, telnet và dns.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Tiếp tục phân tích trên các cổng ứng dụng khác, ta thấy hiện tượng xảy ra tương tự với các cổng ứng dụng 22, 23. Điều này cho thấy máy do thám đã thực hiện hành vi quét cổng với kỹ thuật TCP Connection Scan

A screenshot of a computer

AI-generated content may be incorrect.

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

Dựa vào kết quả quét ở phần 2, hãy lập báo cáo ngắn gọn về các lỗ hổng đã được công bố trên các phần mềm cung cấp dịch vụ. Thông tin về các lỗ hổng có thể tìm kiếm trên <https://www.cvedetails.com/>

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ (tên dịch vụ, tên phần mềm, phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng** |
| Apache HTTP Server 2.4.49 | CVE-2021-41773 | Cho phép thực hiện Local File Inclusion (LFI) |
| OpenSSL 1.0.2g | CVE-2016-2107 | Lỗi padding oracle trong AES CBC ciphers |
| Phần mềm dịch vụ | Số CVE | Mô tả ngắn gọn về lỗ hổng |