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

Tên: Phạm Đình Nam

MSSV: 1050070013

Lớp: 10-TMĐT

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

**1.1. Kịch bản 1**

Terminal 1:

- Kiểm tra ip

A screenshot of a computer program

AI-generated content may be incorrect.

-Truy cập máy ảo

$ sudo wireshark



Terminal 2:

nmap -sn 10.0.2.0/24

A screenshot of a computer

AI-generated content may be incorrect.

Có thể thấy ngoài địa chỉ 10.0.2.1 là địa chỉ của máy tấn công thì còn 3 nút mạng nữa đang hoạt động có địa chỉ là 10.0.2.2, 10.0.2.3 và 10.0.2.15.

- **Phân tích lưu lượng**:

Nguồn phát là máy do thám (PCSSystemec\_04:42:...), gửi các gói ARP broadcast để xác định IP trong dải 10.0.2.0/24.

A screenshot of a computer

AI-generated content may be incorrect.

- Trên cửa sổ của Wireshark, sử dụng giá trị arp.opcode == 2 cho bộ lọc

A screenshot of a computer

AI-generated content may be incorrect.

**Kết quả**: Kỹ thuật quét được sử dụng là ARP Scan. Wireshark cho thấy hàng loạt gói ARP request từ máy do thám đến toàn bộ dải mạng 10.0.2.0/24 và các ARP reply từ các máy đang hoạt động.

**1.2. Kịch bản 2**

nmap -sS -F 10.0.2.3

A screen shot of a computer program

AI-generated content may be incorrect.

**- Phân tích lưu lượng:**

Có các gói **TCP SYN** gửi từ 10.0.2.15 (máy do thám) đến nhiều cổng của 10.0.2.3 (máy mục tiêu).

A screenshot of a computer

AI-generated content may be incorrect.

- Lọc bằng tcp && ip.addr == 10.0.2.3

A screenshot of a computer

AI-generated content may be incorrect.

Tất cả là các gói **SYN** gửi đến nhiều cổng khác nhau

**Kết luận**: Kỹ thuật quét là: TCP SYN Scan.

**1.3. Kịch bản 3**

nmap -sA -F 10.0.2.3

A screen shot of a computer

AI-generated content may be incorrect.

- Phân tích lưu lượng:

Nhiều gói TCP ACK từ máy do thám 10.0.2.15 đến 10.0.2.3. Và phản hồi ICMPtừ 10.0.2.3

A screenshot of a computer

AI-generated content may be incorrect.

- Lọc bằng tcp && ip.addr == 10.0.2.3

A screenshot of a computer

AI-generated content may be incorrect.

**Kết luận**: Kỹ thuật được sử dụng là: TCP ACK Scan

**2. Thu thập thông tin hệ thống**

A screenshot of a computer

AI-generated content may be incorrect.

- Lọc bằng tcp.port == 25

A screenshot of a computer

AI-generated content may be incorrect.

Máy 10.0.2.15 đang **quét toàn bộ dải mạng** 192.168.100.0/24 để kiểm tra máy nào đang mở **dịch vụ email (SMTP – cổng 25)**.

**Kết luận**: máy 192.168.100.59 trong mạng 192.168.100.0/24 đang **chạy dịch vụ email (SMTP)** trên cổng 25.

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

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ**  **(tên dịch vụ, tên phần mềm, phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng (Tiếng Việt)** |
| DNS, BIND 9.11 | CVE-2018-5740 | Lỗ hổng từ chối dịch vụ qua truy vấn DNSSEC gây quá tải tài nguyên |
| HTTP, Apache 2.4.41 | CVE-2021-41773 | Cho phép truy cập trái phép tệp hệ thống qua lỗi path traversal |
| SMTP, Postfix 3.3.0 | CVE-2019-15846 | Cho phép khai thác lỗ hổng xác thực trong Dovecot (thường dùng chung với Postfix), dẫn đến truy cập trái phép |