BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

***Họ và tên sinh viên: Giang Thị Sông Hằng***

***MSSV: 1050080133***

**KẾT QUẢ THỰC HÀNH**

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

* Ảnh chụp kết quả thực hiện của nmap
* A screenshot of a computer

  Description automatically generated

Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng

**A screenshot of a computer

Description automatically generatedHình 1**

A screenshot of a computer

Description automatically generated**Hình 2**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Kỹ thuật thăm dò** | **Đặc điểm lưu lượng quan sát** | **Hình ảnh minh chứng** |
| **1** | TCP SYN Scan | Gói TCP gửi SYN, không hoàn tất 3-way handshake | Hình 1 |
| **2** | ARP Scan | Gói ARP hỏi – đáp trong mạng LAN | Hình 2 |

**1.2 Kịch bản 2**

* Ảnh chụp kết quả thực hiện của nmap:
* A screenshot of a computer

  Description automatically generated
* Phân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng

**Hình 1**

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

**Hình 2**

Dựa trên phân tích gói tin trong Wireshark, có thể xác định hai kỹ thuật thăm dò được sử dụng như sau:

**1. DNS Scan (Hình 1):**

- Đặc điểm: Nhiều gói tin DNS query liên tục từ `10.0.2.15` đến `192.168.0.1`.

- Mục đích: Dò tìm thông tin máy chủ trong mạng thông qua truy vấn tên miền.

- Phân tích: Các truy vấn DNS liên tục thể hiện hành vi quét tìm dịch vụ DNS hoạt động.

**2. TCP SYN Scan (Hình 2):**

- Đặc điểm: Gửi các gói SYN đến nhiều địa chỉ IP và port (443, 80,...), nhận lại gói RST hoặc ACK.

- Mục đích: Dò xem cổng có mở hay không mà không thiết lập kết nối hoàn chỉnh.

- Phân tích: Sự xuất hiện của SYN và phản hồi RST xác nhận kiểu quét Half-open TCP SYN scan.

* 1. **Kịch bản 3**
* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedPhân tích đặc điểm lưu lượng để cho thấy kỹ thuật quét thăm dò là gì? Lưu ý mỗi đặc điểm được chỉ ra phải có hình ảnh chụp màn hình để minh chứng:

**Hình 1**

* \

A screenshot of a computer

Description automatically generated

**Hình 2**

Dựa vào lưu lượng mạng trong Hình 1 và Hình 2, có thể xác định kỹ thuật quét thăm dò được sử dụng là **TCP SYN Scan** (Half-open Scan). Điều này được thể hiện rõ qua chuỗi các gói TCP có cờ SYN đến nhiều cổng đích khác nhau từ máy 10.0.2.15 đến máy 192.168.0.15, mà không có quá trình hoàn tất kết nối TCP.

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)

A screenshot of a computer

Description automatically generated

**Lệnh quét máy chủ email:**

**nmap -sV -p 25,110,143,465,587,993,995 192.168.0.0/24**

Cổng Dịch vụ Giao thức Chức năng

25 SMTP TCP Gửi email từ client → mail server

110 POP3 TCP Nhận email (không bảo mật)

143 IMAP TCP Truy cập email (không bảo mật)

465 SMTPS TCP SMTP bảo mật qua SSL/TLS

587 Submission TCP SMTP gửi email có xác thực

993 IMAPS TCP IMAP bảo mật qua SSL/TLS

995 POP3S TCP POP3 bảo mật qua SSL/TLS

**2.1. Thông tin hệ điều hành:**

* Hình ảnh chụp kết quả của nmap: 0.25 điểm
* A screenshot of a computer

  Description automatically generated

Nêu tên và phiên bản hệ điều hành: 0.25 điểm

**Tên hệ điều hành**: Oracle VirtualBox

**2.2 Thông tin hệ điều hành thu được từ nmap:**

* Địa chỉ IP mục tiêu: 192.168.0.1
* Hệ điều hành đoán được: Oracle VirtualBox (96%)
* Các cổng mở: 22 (SSH), 53 (DNS), 80 (HTTP), 1900 (UPnP)
* Kết luận: Hệ điều hành của máy mục tiêu chạy trong môi trường ảo hóa (VirtualBox hoặc QEMU).
  1. **Thông tin dịch vụ: 1 điểm**
* Hình ảnh chụp kết quả của nmap: 0.25 điểm
* A screenshot of a computer screen

  Description automatically generated
* Danh sách dịch vụ: 0.75 điểm

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
| 1 | SSH | 22 | Dropbear sshd 2020.80 (protocol 2.0) |
| 2 | DNS | 53 | dnsmasq 2.78 |
| 3 | HTTP | 80 |  |
| 4 | UPnP | 1900 | Portable SDK for UPnP devices 1.6.19 (Linux 2.6.36) |

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.

Mỗi lỗ hổng: 1 điểm

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ (tên dịch vụ, tên phần mềm, phiên bản)** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng (Tiếng Việt)** |
| SSH – Dropbear sshd 2020.80 | CVE-2020-36254 | Lỗi tràn bộ đệm trong Dropbear SSH dẫn đến thực thi mã từ xa. |
| DNS – dnsmasq 2.78 | CVE-2020-25681 | dnsmasq dễ bị tấn công DoS do xử lý gói DNS không hợp lệ. |