BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

***Họ và tên sinh viên:Nguyễn Thanh Thản***

***MSSV: 1050070027***

***Lớp:TMĐT***

***Link youtube:*** [***https://youtu.be/3s1v8KP9HCc***](https://youtu.be/3s1v8KP9HCc)

***Link youtube:***

***Link git:*** ***https://github.com/ThanhThan123/test.git***

***Yêu cầu kết quả thực hành:***

Kết quả bỏ vào file word có tên theo định dạng HoTenSV\_MSSV\_Lab07

* Báo cáo kết quả thực hành
* File bắt lưu lượng trên các máy do thám của mỗi kịch bản. Kích thước mỗi file không quá 5MB.

**KẾT QUẢ THỰC HÀNH**

1. **Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**   
   **1.1. Kịch bản 1 (ARP Ping Scan)**

**Lênh -nmap**

* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm
* 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: 1 điểm
* A screenshot of a computer

  AI-generated content may be incorrect.

*Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm*

*Kỹ thuật: ARP ping Scan dùng để dò các hoạt động trong mạng dò host trong mạng Lan mà không cần quét cổng*

A screen shot of a computer screen

AI-generated content may be incorrect.

*Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm*

**1.2. Kịch bản 2 -nmap -nmap -sS -F TCP SYN Scan(half-open scan)**

**Lệnh -nmap -sS -F địa chỉ mạng**

A screenshot of a computer

AI-generated content may be incorrect.

Đặc điểm lưu lượng

+ Thấy nhiều lưu lượng gói TCP STN được gửi từ máy Kali đến mục tiêu

+Một ssố cổng phản hồi bằng Syn/Ack sau đó là RST từ kali huỷ kết nối không thiết lập kết nối hoàn chỉnh

Kỹ thuật quét steath , không thiết lập kết nối TCP

A screenshot of a computer

AI-generated content may be incorrect.

Kỹ thuật quét stelth, không thiết lập kết nối TCP hoàn chỉnh

**1.3. Kịch bản 3**

**Lệnh nmap0 -sA F dia\_chi\_mang**

* Ảnh chụp kết quả thực hiện của nmap: 0.5 điểm

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Đặc điểm lưu lượng:

+ Nmap gửi nhiều gói có TCP flag: ACK đến các cổng đích

+Phản hồi nhậnd dược là TCP RST từ máy mục tiêu

Kỹ thuật là dùng để kiểm tra xem cổng có bị lọc hay không

A screenshot of a computer

AI-generated content may be incorrect.

* 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: 1 điểm

*Nếu không phân tích đúng đặc điểm lưu lượng: 0 điểm*

*Phân tích đúng đặc điểm nhưng nêu sai tên kỹ thuật quét: 0.5 điểm*

1. **Thu thập thông tin hệ thống**

**Lệnh để quét thăm dò tìm kiếm máy chủ email là nmap là**

**Nmap -sV p 25,110,143,465,587,995,192.168.100.0/24**

**Giải thích các tham số**

**-sV: quét phát hiện phiên bản dịch vụ đang chạy trên các cổng mở**

**-p: chỉ định cụ thể các cổng email để quét thay vì quét toàn bộ**

**25**

* 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)

**Thông tin hệ điều hành:**

* Hình ảnh chụp kết quả của nmap: 0.25 điểm
* Nêu tên và phiên bản hệ điều hành: 0.25 điểm

**Thông tin dịch vụ: 1 điểm**

* Hình ảnh chụp kết quả của nmap: 0.25 điểm
* Danh sách dịch vụ: 0.75 điểm

|  |  |  |  |
| --- | --- | --- | --- |
| **ST**  **T** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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)** |
|  |  |  |
|  |  |  |