BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

Họ và tên sinh viên:Nguyễn Minh Nhật Đan

MSSV:1050080046

Lớp : 10\_ĐH\_CNPM1

**KẾT QUẢ THỰC HÀNH**

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

1.1. Kịch bản 1

A screenshot of a computer

AI-generated content may be incorrect.

Thực hiện lệnh nmap -sn 192.168.117.0/24

Kỹ thuật mạng đã tấn công :   
Kỹ thuật PingScan

**1.2. Kịch bản 2**

A screenshot of a computer

AI-generated content may be incorrect.

Dựa trên đặc điểm các gói mạng khi thực hiện nmap gửi một RST để tránh hoàn toàn mất kết nối

-Kỹ thuật này là kỹ thuật quét cổng nửa mở

**1.3. Kịch bản 3**

A screenshot of a computer

AI-generated content may be incorrect.  
Dựa trên đặc điểm gói mạng :   
+Tất cả các lưu lượng gói mạng đều thuộc giao thức TCP   
+Nhiều gói tin có trạng thái RST, ACK : Điều này xảy ra vì kết nối bị từ chối

+Các gói tin hiển thị chỉ kiểm tra trạng thái, nếu bị đóng sẽ trả về RST

-Kỹ thuật tấn công :ACK scan

**2. Thu thập thông tin hệ thống**

Lệnh quét thăm dò tìm kiếm máy chủ email là :

nmap -p 25,110,143,465,587,993,995 192.168.100.0/24

**2. Giải thích các tham số sử dụng trong lệnh**

* nmap: công cụ quét mạng được sử dụng để phát hiện các máy chủ và dịch vụ trên mạng.
* -p: Tham số này chỉ định các cổng cần quét.
  + 25: Cổng SMTP, dùng để gửi email.
  + 110: Cổng POP3, dùng để nhận email.
  + 143: Cổng IMAP, dùng để nhận email.
  + 465: Cổng SMTPS, dùng để gửi email qua SSL/TLS.
  + 587: Cổng SMTP Submission, dùng để gửi email với xác thực.
  + 993: Cổng IMAPS, dùng để nhận email qua SSL/TLS.
  + 995: Cổng POP3S, dùng để nhận email qua SSL/TLS.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Thông tin hệ điều hành:

A screenshot of a computer

AI-generated content may be incorrect.

- Hình ảnh chụp kết quả của nmap: 0.25 điểm

Tên và phiên bản hệ điều hành :Không xác định được

STT Tên dịch vụ Số hiệu cổng ứng dụng Tên phần mềm và phiênbản

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Tên dịch vụ | Số hiệu cổng ứng dụng | Tên phần mềm và phiên bản |
| 1 | SMTP | 25 | Postfix smtpd |
| 2 | IMAP | 143 | Dovecot imapd |
| 3 | HTTP | 80 | Apache httpd 2.4.41 |

3. 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.

|  |  |  |
| --- | --- | --- |
| Phần mềm dịch vụ | Số CVE | Mô tả ngắn gọn về lỗ hỏng |
| Apache httpd 2.4.41 | CVE-2020-11985 | Lỗi trong mã xử lý tiêu đề HTTP dẫn đến việc máy chủ không xử lý đúng các yêu cầu đặc biệt, gây ra crash |
| Postfix | CVE-2020-6104 | Lỗi trong cơ chế xác thực SMTP cho phép kẻ tấn công giả mạo danh tính người gửi. |
| Dovecot | CVE-2020-25275 | Lỗi trong mã xử lý TLS dẫn đến việc tiêu tốn tài nguyên khi bị khai thác. |
| Dovecot (IMAP, Dovecot imapd) | CVE-2020-25275 | Lỗi trong xử lý TLS, gây tiêu tốn tài nguyên và dẫn đến từ chối dịch vụ. |