BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

**Họ và tên sinh viên:** Trần Thiên Nam

**MSSV:** 1050080275

**Lớp:** CNPM3\_10\_ĐH

Bài Làm

**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.**

Câu lệnh: nmap -sn 192.168.2.253/24

Chi tiết:  
 -sn - Tag này được sử dụng để quét các IP mà không cần quét cổng

Kết quả:

* Đã quét được từ 192.168.2.0 đến 192.168.2.255
* Đã có ít nhất 50 thiết bị được kết nối mạng trong mạng nội bộ

**1.2. Kịch bản 2:**

A screenshot of a computer

AI-generated content may be incorrect.

Như các đợt quét mạng ở trên cho thấy có ít nhất 50 thiết bị kết nối mạng. Chúng ta đi thực hiện kiểm tra các dịch vụ gì đang chạy trên ip: 192.168.2.12

Câu lệnh: nmap -sS 192.168.2.12

Chi tiết:  
 -sS - Tag này được sử dụng để quét các IP trong Nmap gọi là TCP SYN scan

Kết quả:

* Host is up: Thiết bị tại IP 192.168.2.12 đang hoạt động (ping được).
* 992 filtered tcp ports: 992 cổng không phản hồi → bị lọc (filtered) bởi firewall hoặc không mở.
* **8 cổng mở (open)** được liệt kê chi tiết bên dưới:

|  |  |  |  |
| --- | --- | --- | --- |
| **Cổng** | **Trạng thái** | **Dịch vụ liên quan** | **Mô tả ngắn** |
| 135/tcp | open | msrpc | Remote Procedure Call (dùng bởi Windows services) |
| 139/tcp | open | netbios-ssn | NetBIOS Session Service (chia sẻ file/printer) |
| 445/tcp | open | microsoft-ds | SMB over TCP (chia sẻ file trong Windows) |
| 902/tcp | open | iss-realsecure | VMware Server Remote Management (thường gặp) |
| 2382/tcp | open | ms-olap3 | Dịch vụ SQL Server Analysis Services |
| 3306/tcp | open | mysql | MySQL database |
| 5357/tcp | open | wsdapi | Web Services for Devices (thường thấy ở Windows) |
| 8080/tcp | open | http-proxy | Web server, thường dùng làm reverse proxy/test site |

**1.3. Kịch bản 3:**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

Câu lệnh:

nmap -p- 192.168.2.12

tshark

Chi tiết:  
 -p- - Tag này được sử dụng để quét tất cả các ports trong Nmap gọi là TCP SYN scan

Kết quả:

* Nmap đang quét tất cả các ports từ 1 -> 65565
* Cho thấy nmap đang tích cực quét các ports trên địa chỉ 192.168.2.12 thông qua ip của máy Kali Linux là: 192.168.198.133

A screenshot of a computer

AI-generated content may be incorrect.

**2. Thu thập thông tin hệ thống**

Để quét và tìm kiếm máy chủ email (SMTP server) trên một hệ thống, ta có thể dùng lệnh nmap với mục tiêu là các cổng dịch vụ email phổ biến như:

* 25 (SMTP)
* 465 (SMTPS – SMTP over SSL)
* 587 (SMTP – Submission)

A screenshot of a computer

AI-generated content may be incorrect.

Câu lệnh: nmap -sS -O -p 25,465,587 -sV 192.168.2.12

Chi tiết:  
 -sS - Tag này được sử dụng để quét trong Nmap gọi là TCP SYN scan

-O - Tag này Bật tính năng phát hiện hệ điều hành (OS Detection). Nmap sẽ cố gắng phân tích dấu hiệu TCP/IP stack để đoán hệ điều hành và phiên bản.

-p 25,245,587 - Như đã nêu ở trên thì để quét máy chủ email (SMTP server) trên một hệ thống.

-sV - Chỉ định input sau đó cho một địa chỉ hay domain cần kiểm tra.

Kết quả:

* Máy đến có hoạt động và phản hồi.
* Các cổng email đã bị lọc:

A black background with white text

AI-generated content may be incorrect.

Ba cổng thường dùng cho SMTP (gửi email) đều ở trạng thái filtered, nghĩa là:

* Nmap không nhận được hồi đáp từ các cổng này.
* Có thể là firewall đang chặn hoặc drop các gói tin quét.
* Không xác định được phiên bản dịch vụ (vì không có phản hồi).
* Hệ thống được ghi nhận là sử dụng windows XP|7|2012 có thể đang chạy trong máy ảo VMWare. Tuy nhiên có dòng cảnh báo không chắn cho cho việc này: `*Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port*`

A screen shot of a computer

AI-generated content may be incorrect.

Danh sách các dịch vụ đã quét được:

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Số hiệu cổng ứng dụng** | **Tên phần mềm và phiên bản** |
| 1 | smtp | 25/tcp | windows XP|7|2012 |
| 2 | smtps | 465/tcp | windows XP|7|2012 |
| 3 | submission | 587/tcp | windows XP|7|2012 |

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

Sử dụng:

nmap -sS -sV -O -Pn 192.168.2.12

nmap --script vuln 192.168.2.12

Để: Thu thập thông tin

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Từ kết quả này, ta có thể rút ra rất nhiều thông tin quan trọng về mục tiêu 192.168.2.12:

Tình trạng hệ thống:

* Máy chủ đang hoạt động với độ trễ rất thấp: 0.00081s latency
* Có nhiều cổng mở cung cấp các dịch vụ có thể bị khai thác

**Các dịch vụ đang mở và nhận diện được phiên bản:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Cổng** | **Trạng thái** | **Dịch vụ** | **Phiên bản phát hiện** |
| 135 | open | msrpc | Microsoft Windows RPC |
| 139 | open | netbios-ssn | Microsoft Windows NetBIOS |
| 445 | open | microsoft-ds? | Chưa xác định rõ phiên bản – thường là SMB |
| 902 | open | ssl/vmware-auth | VMware Authentication Daemon 1.10 |
| 2382 | open | ms-olap3? | Có thể là dịch vụ Microsoft OLAP |
| 3000 | open | http | Grafana http – dịch vụ hiển thị dashboard dữ liệu |
| 3306 | open | mysql | Có MySQL, nhưng không cho phép truy cập (unauthorized) |
| 5357 | open | http | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) – dịch vụ hệ điều hành |
| 5432 | open | postgresql | PostgreSQL từ phiên bản 9.6.0 trở lên |
| 8000 | open | http | Apache httpd 2.4.54 ((Win64) OpenSSL/1.1.1p) |
| 8080 | open | http | Apache httpd – có thể là ứng dụng web nội bộ khác |

Hệ điều hành được suy đoán:

* Microsoft Windows XP SP3, hoặc
* Windows 7, hoặc
* Windows Server 2012
* Có dấu hiệu chạy trên máy ảo VMware Player

Ngoài ra: Nmap báo cảnh báo "OSScan results may be unreliable", do không phát hiện được đủ cổng open/closed để xác định OS chính xác hơn.

Tóm tắt mức độ rủi ro:

* Cổng 445 (SMB) mở → có thể bị tấn công bằng EternalBlue nếu chưa được vá.
* Cổng 3306 (MySQL) và 5432 (PostgreSQL) đang mở → dễ bị dò mật khẩu hoặc tấn công SQL nếu không bảo vệ đúng cách.
* Grafana trên cổng 3000 → nếu không có auth mạnh, có thể bị xem dashboard hoặc RCE.

**Từ đó ta đã có các danh sách sau:**

|  |  |  |
| --- | --- | --- |
| **Phần mềm dịch vụ** | **Số CVE** | **Mô tả ngắn gọn về lỗ hổng** |
| Apache HTTP Server 2.4.54 (Win64, OpenSSL 1.1.1p) | CVE-2022-31813 | Lỗi xử lý sai input trong mod\_proxy có thể bị khai thác để bypass security policy. |
| Grafana HTTP (port 3000) | CVE-2021-43798 | Lỗi path traversal cho phép truy cập file nội bộ trái phép trên hệ thống. |
| PostgreSQL 9.6.x | CVE-2018-1058 | Cho phép tấn công mở rộng đặc quyền khi kết nối database không bảo vệ kỹ quyền user. |
| Microsoft SMBv1 (port 445 - Windows XP/7/2012) | CVE-2017-0144 | Lỗ hổng EternalBlue cho phép thực thi mã từ xa, bị khai thác bởi ransomware WannaCry. |