BÁO CÁO THỰC HÀNH

**Bài thực hành số 04**

**QUÉT LỖ HỔNG BẢO MẬT**

|  |  |
| --- | --- |
| **Môn học:** An toàn Mạng máy tính | **Điểm tự đánh giá** |
| **Lớp:** NT101.N11.1  **Giảng viên hướng dẫn:** Văn Thiên Luân | **10** |

**PHÂN CÔNG NHIỆM VỤ NHÓM 1:**

|  |  |  |
| --- | --- | --- |
| **MSSV** | **Họ và Tên** | **Nhiệm vụ** |
| 20521086 | Trang Kỳ Anh | Họp làm chung tất cả các bài |
| 20521280 | Lê Thanh Hằng |
| 20520131 | Dương Đức Anh |

**ĐÁNH GIÁ KHÁC:**

|  |  |
| --- | --- |
| Tổng thời gian thực hiện | 60 tiếng |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị | - Máy ảo hay lỗi mạng nên phải làm chung  - Tốn nhiều thời gian để sửa mạng cho máy ảo  - Bài thực hành viết bằng tiếng anh gây một chút khó khăn trong việc đọc – hiểu một số thuật từ. |

**MỤC LỤC**

[A. BÁO CÁO CHI TIẾT 3](#_Toc120898060)

[**I.** **Quét lỗ hổng sử dụng công cụ Nessus** 3](#_Toc120898061)

[1. Quét máy Metasploitable 2 không sử dụng tài khoản chứng thực 3](#_Toc120898062)

[2. Bật Wireshark sau đó tiến hành quét và xác định các bước mà Nessus đã thực hiện hoàn thành quá trình quét 7](#_Toc120898063)

[3. Quét không chứng thực có sử dụng UDP 8](#_Toc120898064)

[4. Quét lỗ hỏng có chứng thực 9](#_Toc120898065)

[5. So sánh quét có chứng thực và không chứng thực 10](#_Toc120898066)

[6. Liệt kê ưu nhược điểm quét có chứng thực và không chứng thực 10](#_Toc120898067)

[7. Quét lại máy Metasploitable2 có sử dụng plugin NFS Exported Share Information Disclosure 10](#_Toc120898068)

[8. Chạy wireshark trong suốt quá trình scan sử dụng 1 plugin duy nhất 11](#_Toc120898069)

[9. Mô tả cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định? 12](#_Toc120898070)

[10. Thực hiện quét sử dụng các pluggin khác 12](#_Toc120898071)

[**II.** **Bài tập nhóm** 14](#_Toc120898072)

[11. Sinh viên/nhóm sinh viên tìm hiểu 1 trong các công cụ quét lỗ hổng tự động sau đây và viết báo cáo kết quả theo như các phần đã chia ở bài 1. 14](#_Toc120898073)

[B. TÀI LIỆU THAM KHẢO 19](#_Toc120898074)

1. **BÁO CÁO CHI TIẾT**
2. **Quét lỗ hổng sử dụng công cụ Nessus**
3. **Quét máy Metasploitable 2 không sử dụng tài khoản chứng thực**
4. Cài đặt Nesuss

* Kiểm tra giá trị checksum trên trang chủ



* Kiểm tra tính toàn vẹn của tập tin Nessus sau khi tải về

Text

Description automatically generated

* Cài đặt Nessus

Text

Description automatically generated

* Khởi động dịch vụ nessusd

Text

Description automatically generated

* Cài đặt và tạo tài khoản Nessus thành công

Graphical user interface, website

Description automatically generated

1. Khai báo đối tượng

* Tạo và cấu hình máy scan Metasploitable 2 với templates Basic Network Scan

Graphical user interface, application

Description automatically generated

1. Cấu hình định nghĩa quét

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

1. Quét lỗ hỏng không sử dụng chứng thực

Graphical user interface, application

Description automatically generated

* 1 host được phát hiện: **Metasploitable** có ip **192.168.111.150** (có 70 lỗ hỏng được phát hiện)

Graphical user interface, text, application

Description automatically generated

* Danh sách lỗ hỏng sau khi được phân loại nhóm

Graphical user interface, text, application, email

Description automatically generated

1. **Bật Wireshark sau đó tiến hành quét và xác định các bước mà Nessus đã thực hiện hoàn thành quá trình quét**

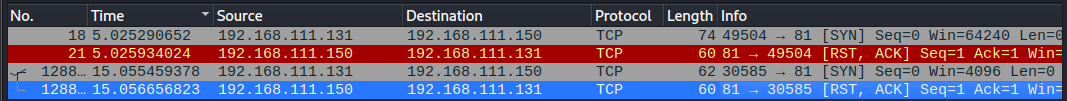
* Nessus thực hiện bắt tay 3 bước với từng port.
* Nếu port nào nhận được tín hiệu chấp nhận trao đổi thì Nessus sẽ gởi gói tin trao đổi thông tin.
* Metasploitable2: 192.168.111.150
* Kali Linux: 192.168.111.131

Port 80

Table

Description automatically generated with low confidence

Port 81



Port 8009

A picture containing calendar

Description automatically generated

1. **Quét không chứng thực có sử dụng UDP**

* Danh sách các lỗ hỏng sau khi scan: có 69 lỗ hỏng

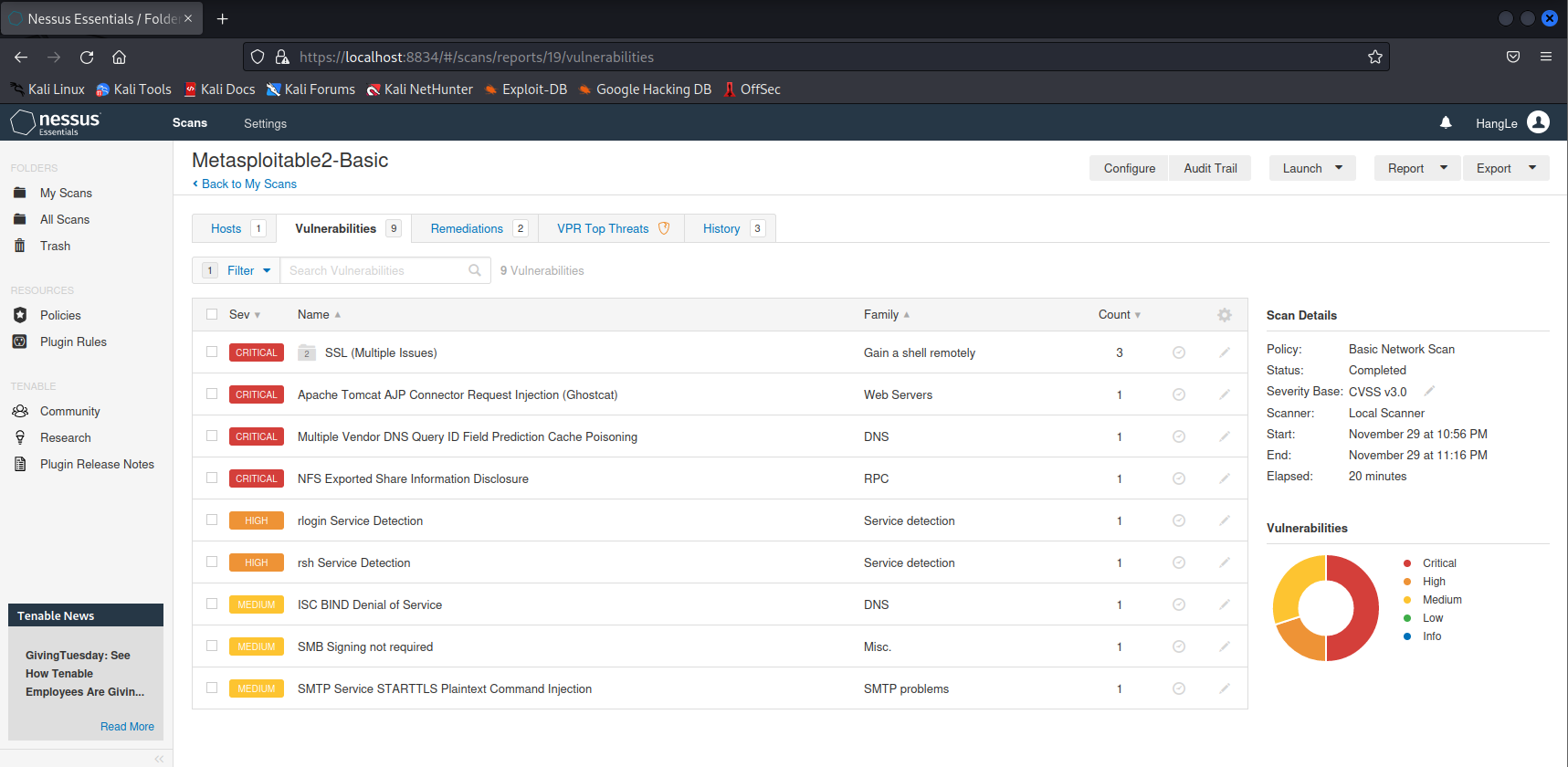
Graphical user interface

Description automatically generated with medium confidence

Graphical user interface

Description automatically generated

* Các lỗ hỏng sau khi được phân loại nhóm



**=> Scan lỗ hỏng không chứng thực có UDP phát hiện ít lỗ hỏng hơn scan không chứng thực không UDP**

1. **Quét lỗ hỏng có chứng thực**

* Tạo và cấu hình máy scan Metasploitable 2 với templates Credentialed Patch Audit
* Kết quả sau khi scan

Graphical user interface

Description automatically generated with medium confidence

* Danh sách các lỗ hỏng sau khi scan

Graphical user interface, text

Description automatically generated

1. **So sánh quét có chứng thực và không chứng thực**

Quét sử dụng tài khoản chứng thực trả về nhiều thông tin cũng như lỗ hổng bảo bảo mật hơn, và cũng tốn ít thời gian hơn so với không chứng thực (19 phút so với 21 phút).

1. **Liệt kê ưu nhược điểm quét có chứng thực và không chứng thực**

Sử dụng tài khoản chứng thực giúp Nessus có thể scan tìm ra lỗi từ bên trong, từ đó trả về nhiều lỗ hổng bảo mật hơn.

Tuy nhiên, basic scan có thể tìm thấy những lỗ hổng thông qua việc nhìn từ góc nhìn bên ngoài ví dụ như lộ thông tin ra ngoài từ các port được mở, thứ mà quét dùng tài khoản chứng thực không phát hiện ra.

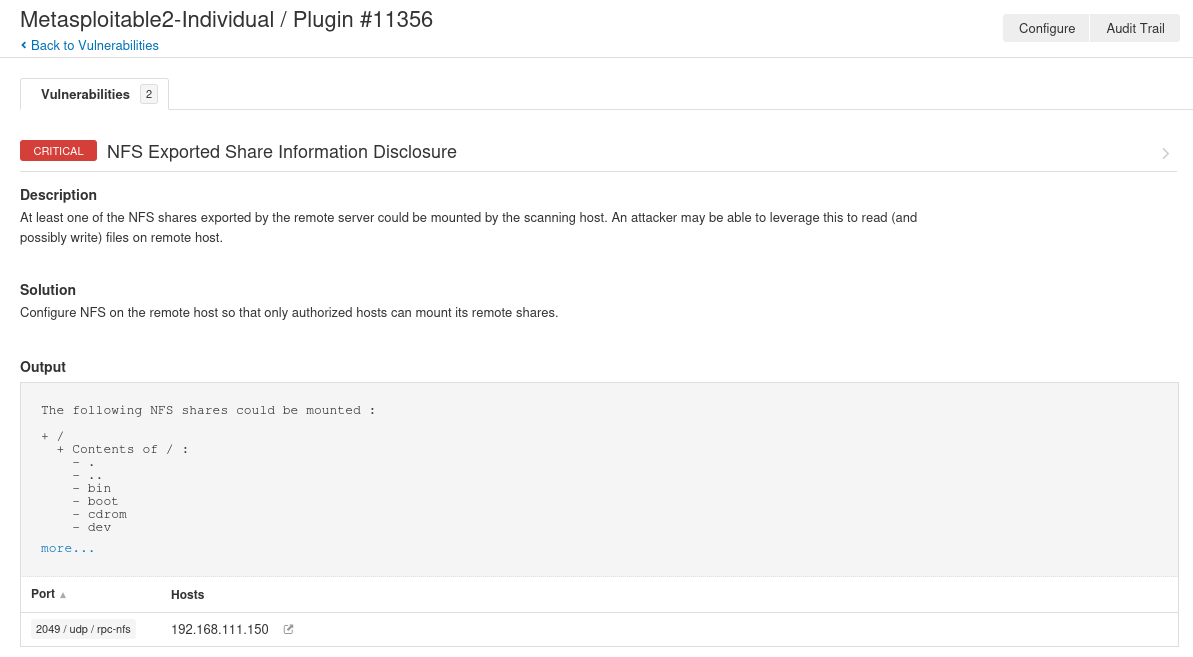
1. **Quét lại máy Metasploitable2 có sử dụng plugin NFS Exported Share Information Disclosure**

* Tạo và cấu hình máy scan Metasploitable 2 với templates Advanced Scan
* Tắt host discovery và các port không cần thiết, sử dụng port 111 để scan
* Kết quả sau khi scan

Graphical user interface

Description automatically generated

* Thông tin lỗ hỏng



1. **Chạy wireshark trong suốt quá trình scan sử dụng 1 plugin duy nhất**

Table

Description automatically generated

Liệt kê các port khác mà Nessus thực hiện scan, không phải port 111? Giải thích tại sao lại scan các port khác khi chỉ sử dụng duy nhất port 111?

* Wireshark trong quá trình chạy bắt được 354 gói tin, trong đó các port scan ngoài 111 là 81, 8009, 80, 161, 445, 139, 8045, 8611, 23, 139, 2810, 7627, …
* Port scan range chỉ dùng để quét những cổng network-based, không phải những cổng local.
* Nếu khi quét tìm thấy cổng đang được mở, kể cả nó không trong port scanning range, nó vẫn sẽ thêm cổng vào vùng quét, chỉ cần các plugins được bật.

1. **Mô tả cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ định?**

Khi đánh giá mục tiêu bằng máy quét mạng như Nessus, một câu hỏi thường gặp là "Làm cách nào để kiểm soát các cổng mà Nessus kiểm tra trong quá trình quét?" Bài báo cáo của nhóm sẽ chỉ ra một số tùy chọn để thực hiện việc này, bao gồm:

* Hạn chế việc quét cổng.
* Chọn kiểu liệt kê máy chủ.
* Xem xét các cổng chưa quét đã đóng.
* Định địa chỉ các cổng UDP.
* Kiểm soát cổng rõ ràng.
* Các tùy chọn thay thế để quét cổng.

1. **Thực hiện quét sử dụng các pluggin khác**

* Chọn các Plugin

Table

Description automatically generated

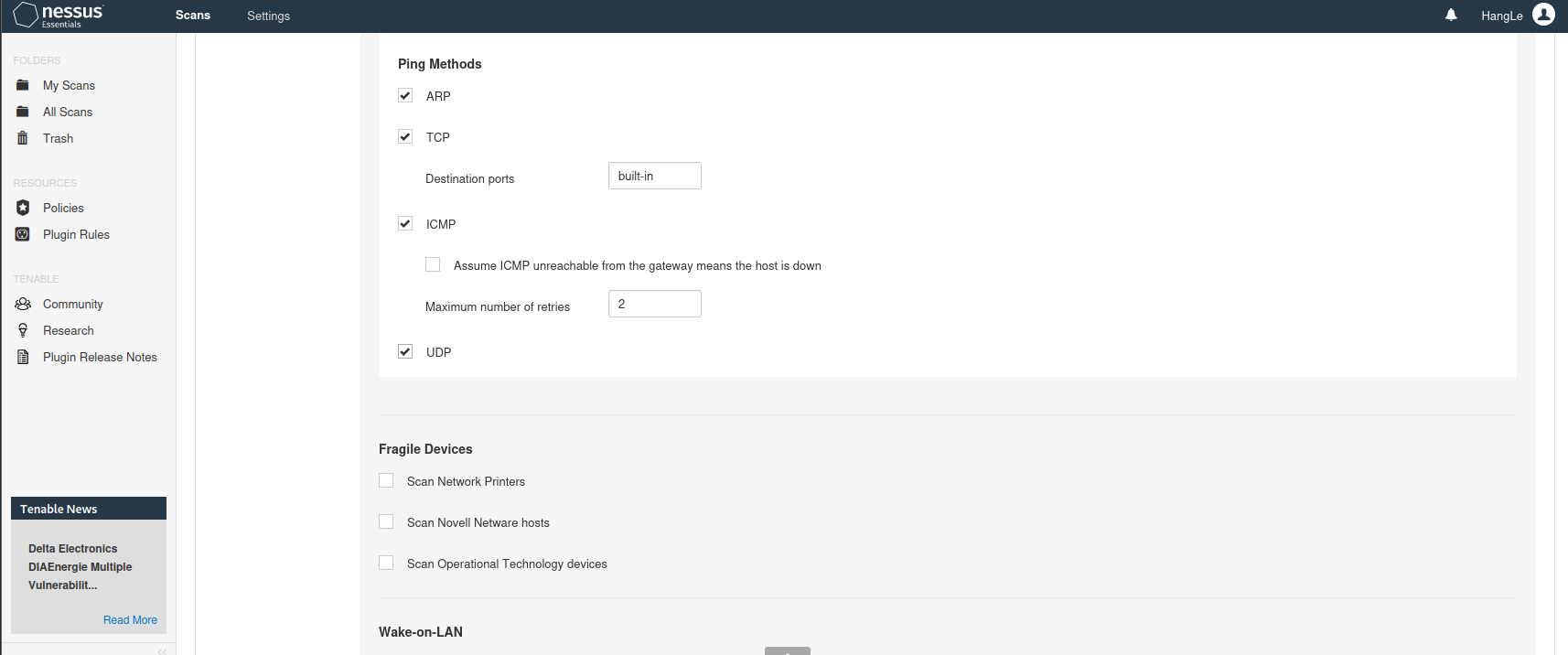
Graphical user interface, table

Description automatically generated

* Config như sau

Graphical user interface, application

Description automatically generated



* Chạy quét

Graphical user interface, application, Teams

Description automatically generated

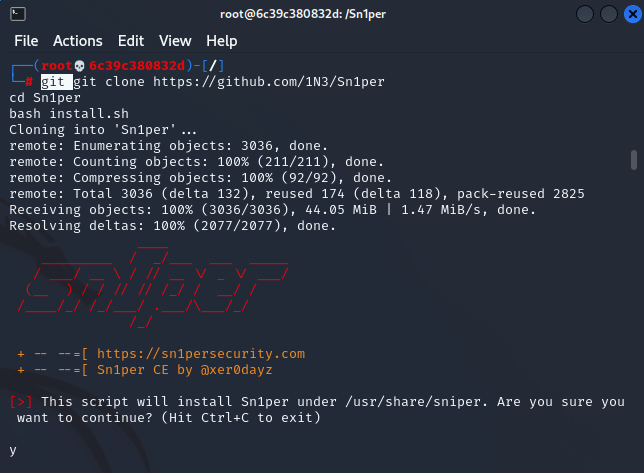
* Kết quả quét

Graphical user interface, text, application, email

Description automatically generated

1. **Bài tập nhóm**
2. **Sinh viên/nhóm sinh viên tìm hiểu 1 trong các công cụ quét lỗ hổng tự động sau đây và viết báo cáo kết quả theo như các phần đã chia ở bài 1.**

* Cài đặt Sn1per



Text

Description automatically generated

* Sử dụng lệnh **sniper -t 192.168.111.150** để quét máy Metasploitable

Text

Description automatically generated

* Chạy xong thu được kết quả

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

1. **TÀI LIỆU THAM KHẢO**