BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng**

**Tên chủ đề: Vuln scaning**

*GVHD: Tô Trọng Nghĩa*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: XXX

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Email |
| 1 | Nguyễn Đình Luân | 21521105 | 21521105@gm.uit.edu.vn |
| 2 | Trần Thanh Triều | 21522713 | 21522713@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung | Tình trạng | Trang |
| 1 | Câu 1-11 | 80% |  |
| Điểm tự đánh giá | | | **7/10** |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

## 1. Thực hiện lại các bước trên để quét máy Metasploitable 2 không sử dụng tài khoản

## chứng thực.

A screenshot of a computer

Description automatically generated

IP của metasploitable: 192.168.5.133

Quét lỗ hổng không sử dụng tài khoản chứng thực

Khai báo đối tượng:

A screenshot of a computer

Description automatically generated

Cấu hình các định nghĩa quét

Cấu hình scanner để quét tất cả các port

A screenshot of a computer

Description automatically generated

Kết quả quét

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Áp dụng filters:

A screenshot of a computer

Description automatically generated

2. Bật Wireshark sau đó tiến hành quét và xác định các bước mà Nessus đã thực hiện

để hoàn tất quá trình quét.

A screen shot of a computer

Description automatically generated

Có thể thấy được là quá trình bắt tay ba bước đã được diễn ra:

Địa chỉ 192.168.179.129 gửi gói tin SYN đến 192.168.179.133 để bắt đầu quá trình bắt tay 3 bước

Bên địa chỉ 192.168.179.133 gửi lại gói tin SYN ACK

Cuối cùng địa chỉ 192.168.179.129 đã gửi gói tin ACK để hoàn thành quá trình bắt tay

Trường hợp khác:



Địa chỉ 192.168.5.129 gửi đến địa chỉ 192.168.5.133 gói tin SYN

Địa chỉ 192.168.5.133 phản hồi gói tin RST ACK để yêu cầu đóng kết nối với flag RST

cho thấy máy có địa chỉ 192.168.5.133 không mở port 90

3. Quét lại nhưng quét thêm port UDP

Add thêm UDP

A screenshot of a computer

Description automatically generated

Kết quả không thấy sự khác biệt

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

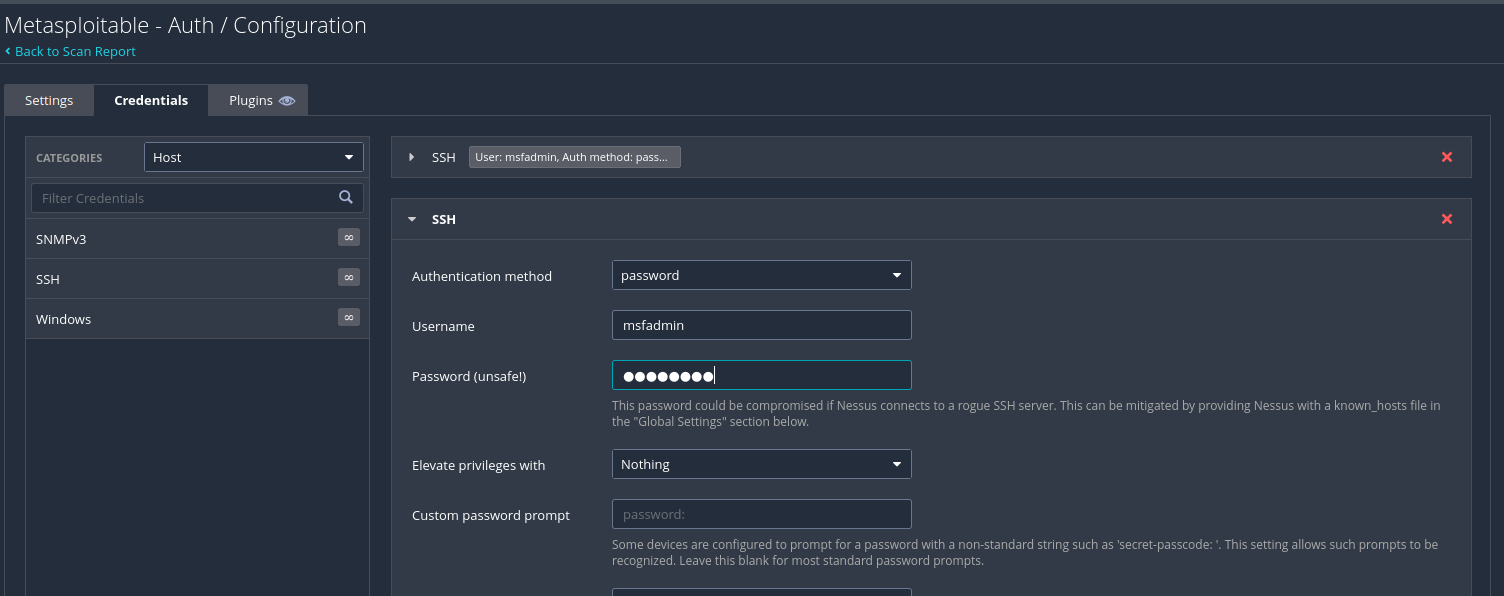
4. Thực hiện lại các bước trên để quét máy Metasploitable 2 có sử dụng tài khoản

chứng thực.

Set up

A screenshot of a computer

Description automatically generated



Kết quả:

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

5. Kiểm tra kết quả quét và so sánh với việc quét không sử dụng tài khoản chứng thực.

Có chứng thực:

A screen shot of a computer

Description automatically generated

Không chứng thực:

A screenshot of a computer

Description automatically generated

Từ hai kết quả trên ta có thể thấy được rằng là được rằng là ở trường hợp khi được cung cấp thêm user id và password thì ta có nhiều quyền truy cập hơn và từ đó có thể thực hiện quét được nhiều lỗi hơn. Các chỉ số critical, high, medium, low có số lượng tăng đáng kể. Điều này chứng tỏ được rằng việc được hỗ trợ user iD và pass có thể hỗ trợ một phần nào đó tốt hơn trong việc phát hiện lỗi.

6. Hãy liệt kê các ưu, nhược điểm khi quét có tài khoản chứng thực và không có tài

khoản chứng thực

Không có tài khoản chứng thực:

Ưu điểm:

+ Không cần hỗ trợ userID và password

+ Có thể kiểm tra được các applications (plugin cục bộ)

Nhược điểm:

+ Không thể kiểm tra được các plugin ngoài cục bộ

+ Kiểm tra thấy được ít lỗi hơn việc không sử dụng tài khoản chứng thực

Có tài khoản chứng thực:

Ưu điểm:

+ Có thể kiểm tra được các application ngoài cục bộ

+ Kiểm tra được nhiều lỗi hơn không có tài khoản chứng thực

Nhược điểm:

+ Cần phải có các cơ chế authenticate

7. Thực hiện lại các bước trên để quét máy Metasploitable 2 sử dụng plugin NFS

Exported Share Information Disclosure

Set up:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Kết Quả: A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

8. Chạy Wireshark hoặc tcpdump trong suốt quá trình scan sử dụng 1 plugin duy nhất.

Liệt kê các port khác mà Nessus thực hiện scan, mà không phải port 111? Tại sao

Nessus lại scan các port khác, trong khi chúng ta đã chỉ định chỉ scan duy nhất 1 port là

111?

Kết quả:

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Có kèm file pcap

Các port ngoài port 111 được sử dụng là: 21, 23, 79, 80, 81,135, 139, 161, 280, 389, 443, 445, 631, 636, 2002, 2049, 2148, 2810, 3268, 3269, 7627, 8009, 8045, 8611, 9000, 9100, 9101, 9200, 10000, 10001, 43737.

Lý do: có nhiều plugins kiểm tra trạng thái của các cổng hardcored mặc định, các port ngoàichỉ định chưa được quét sẽ có trạng thái chưa biết nên get\_port\_state() sẽ trả về True(mặc định). Điều này dẫn đến các port này sẽ bị kết nối thử.

(https://community.tenable.com/s/article/Why-Is-Nessus-Scanning-Ports-Outside-

Of-The-Port-Range)

9. Mô tả cách làm để ngăn chặn việc Nessus scan port khác không phải là port được chỉ

định?

Để ngăn chặn việc Nessus scan các port khác ngoài những port được chỉ định, ta đánh

tick vào lựa chọn “Consider unscanned ports as closed”, khi làm vậy, đối với những

port có trạng thái unknown. get\_port\_state() sẽ trả về FALSE

A screenshot of a computer

Description automatically generated

10.Thực hiện quét lại sử dụng 2 plugin khác.

Plugin 1:

A screenshot of a computer

Description automatically generated

Kết quả:

A screenshot of a computer

Description automatically generated

Plugin 2:

A screenshot of a computer

Description automatically generated

Kết quả:

A screenshot of a computer

Description automatically generated

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 tập 1

Chọn Sn1per

Tiến hành clone và cài đặt:

A screenshot of a computer

Description automatically generated

Chạy chỉ với ip được cung cấp

A screenshot of a computer program

Description automatically generated

Do em lỡ bấm Ctrl+c lúc quét gần xong nên không có report

Scan cổng 80:

A screenshot of a computer program

Description automatically generated

Report:

A screenshot of a computer

Description automatically generated

Có kèm report trong file báo cáo

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)