Bộ môn An toàn Thông tin – Khoa MMT&TT
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

Môn học: An toàn mạng máy tính

Kỳ báo cáo: Buổi 03 (Session 03)

Tên chủ đề: Quét lỗ hổng bảo mật

GV: Trần Nguyễn Đức Huy

Ngày báo cáo: 24/11/2022

Nhóm: 05

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N12.ATCL.1

STT	Họ và tên	MSSV	Email
1	Vũ Hoàng Thạch Thiết	20521957	20521957@gm.uit.edu.vn
2	Nguyễn Hùng Thịnh	20521963	20521963@gm.uit.edu.vn
3	Dương Đỗ Khoa	20521465	20521465@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	Câu 11	60%

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

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

MỤC LỤC

A. BÁO CÁO CHI TIẾT

Câu 1:

Câu 2:

Câu 3:

Câu 4:

Câu 5:

Câu 6:

Câu 7:

Câu 8:

Câu 9:

Câu 10:

Câu 11:

Câu hỏi:

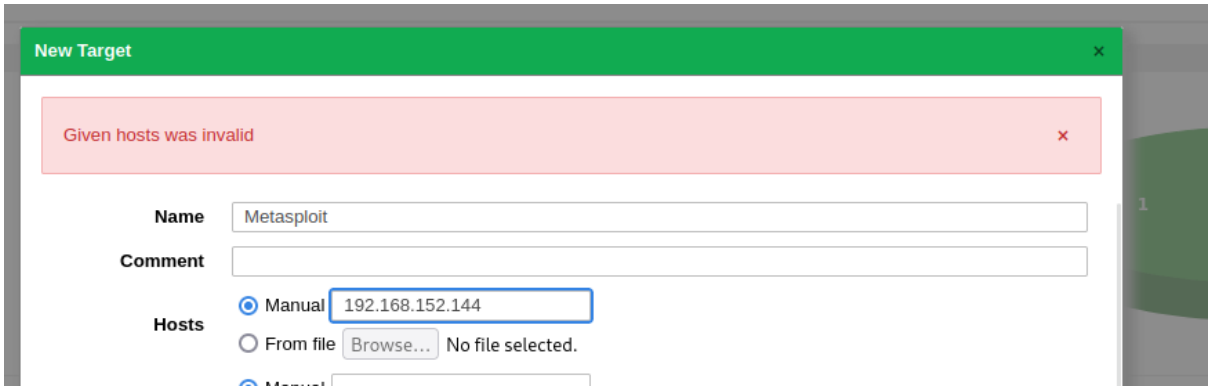
Sinh viên/nhóm sinh viên tìm hiểu 1 trong các công cụ quét lỗ hổng tự động sau đây, và viết báo cáo kết quả theo như các phần đã chia ở bài tập 1:

OpenVAS (https://www.openvas.org/)

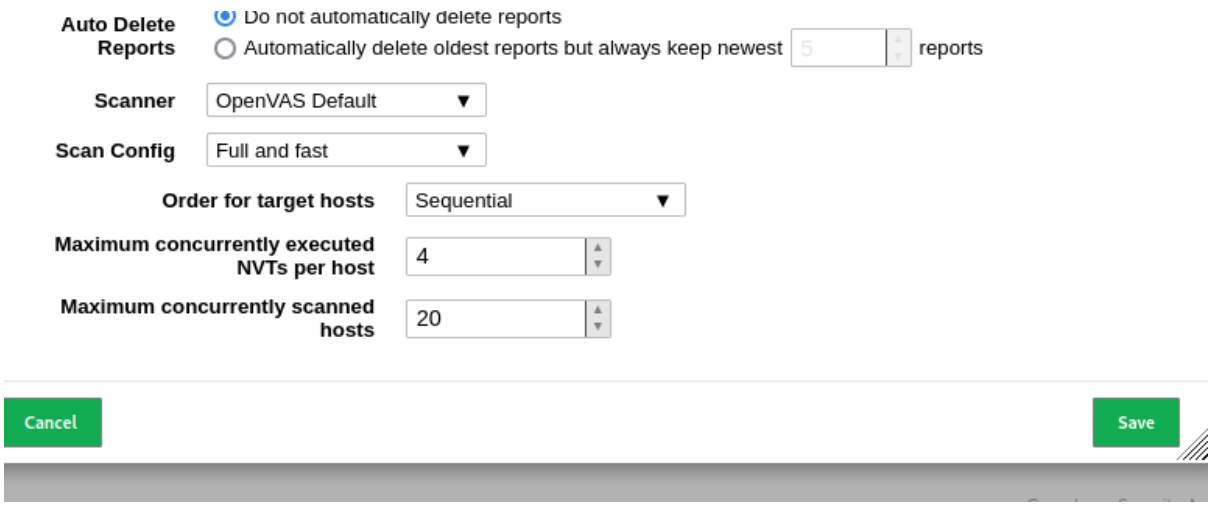
- Tsunami (https://github.com/google/tsunami-security-scanner)
- Rapid7 Nexpose (https://www.rapid7.com/try/nexpose/)
- Qualys Community Edition (https://www.qualys.com/community-edition/)
- Arachni (https://www.arachni-scanner.com/)
- Sn1per (https://github.com/1N3/Sn1per)
- Trivy (https://github.com/aquasecurity/trivy)
- Jok3r (https://github.com/koutto/jok3r)

Trả lời:
Sử dụng công cụ OpenVAS:

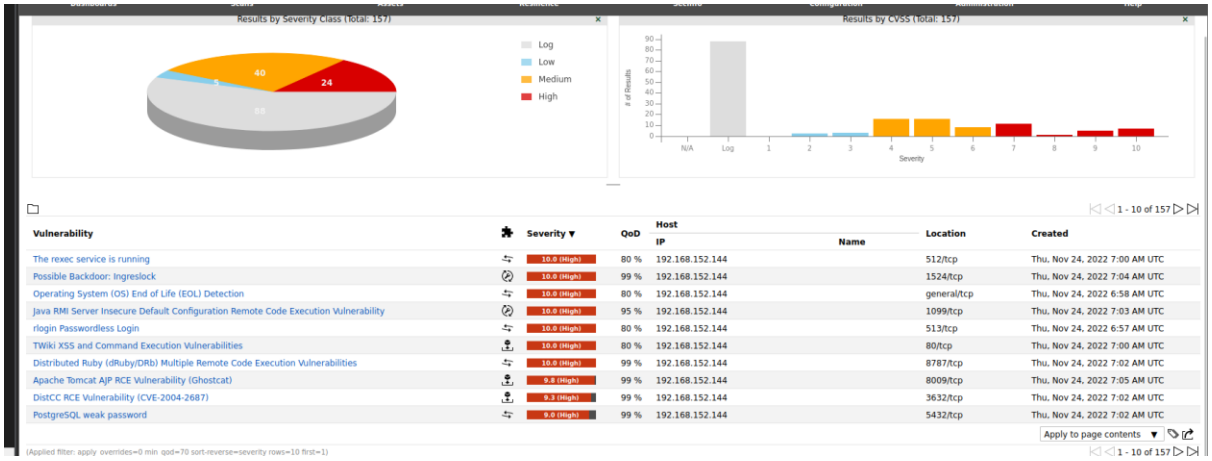
Câu 11.1: Scan không sử dụng tài khoản chứng thực



- Đặt tên cho target và địa chỉ ip là của máy target

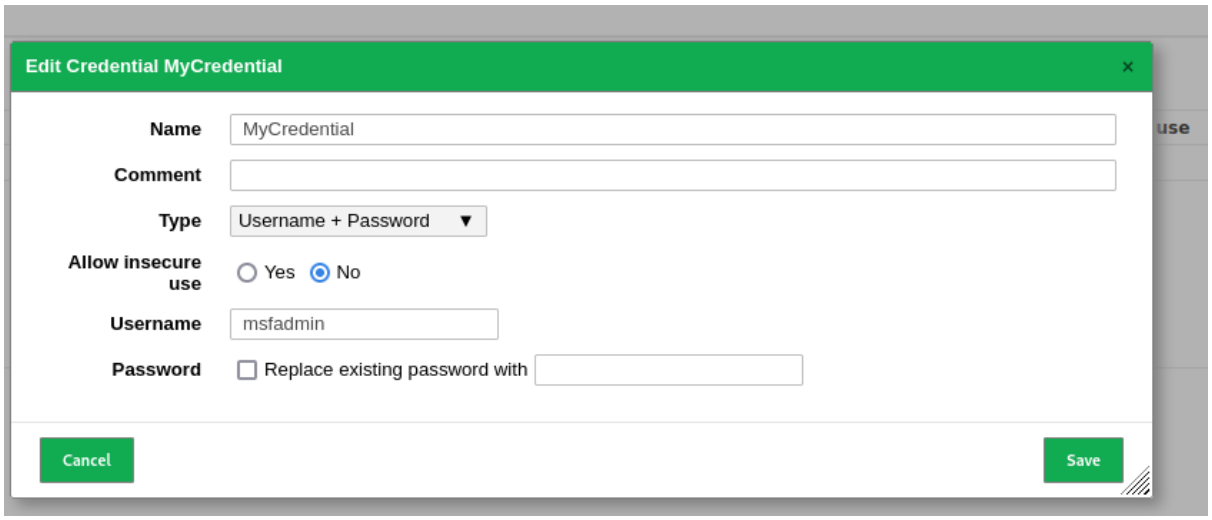


- Scanner ta chọn của openvas default
- Scan config ta chọn full and fast
- Sau đó lưu lại

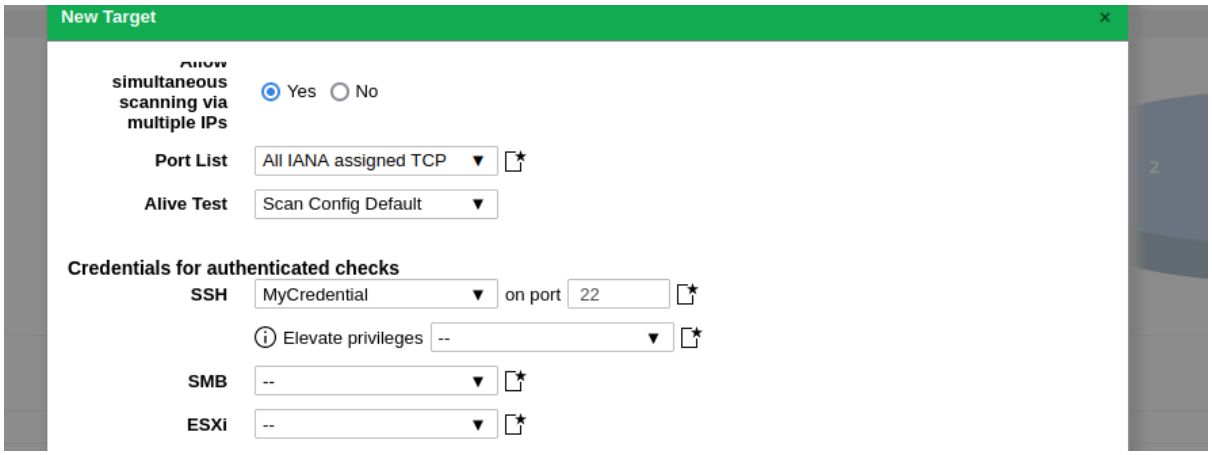


- Kết quả khi quét có khá nhiều lỗ hổng ở mức high

Câu 11.4: Scan sử dụng tài khoản chứng thực

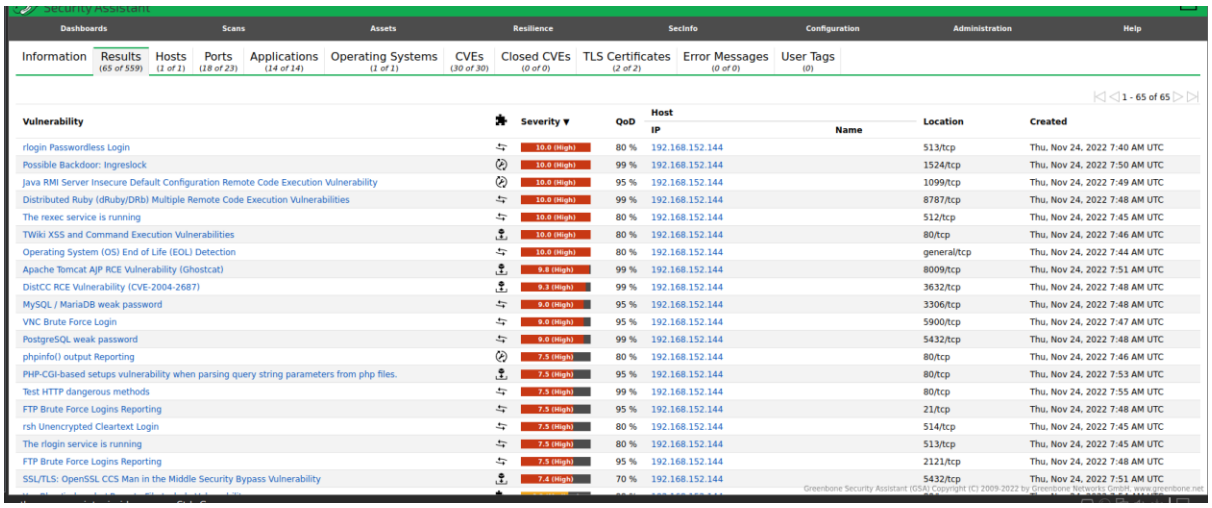


- Trong tab configure chọn Credential
- Tạo mới credential đặt tên
- Chọn type là username+password
- Điền username và password của máy metasploit



- Trong phần task scan ở phần new targer

- Ở phần credential ta chọn credential ta đã tạo sau đó save và scan



- Kết quả khi scan ta thấy có nhiều lỗ hổng hơn so với không có credential

Câu 11.7: Scan với plugin NFS Exported Share Information Disclosure.

Do không tìm thấy filter Plugin nên nhóm em chưa làm được câu 7 trong OpenVAS.

B. TÀI LIỆU THAM KHẢO

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

  *Ví dụ: [*NT101.K11.ANTT*]-Session1_Group3.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT