BÁO CÁO THỰC HÀNH

**Môn học: An toàn Mạng**

**Kỳ báo cáo: Buổi 03 (Session 03)**

**Tên chủ đề: Quét lỗ hổng phần mềm**

*GVHD: Nghi Hoàng Khoa*

*Ngày báo cáo:*

**Nhóm: 07 (ghi số thứ tự nhóm)**

1. **THÔNG TIN CHUNG:**

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

Lớp: NT140.O11.ANTN.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Phạm Ngọc Thơ | 21522641 | 21522@gm.uit.edu.vn |
| 2 | Hà Thị Thu Hiền | 21522056 | 21522056@gm.uit.edu.vn |

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

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Yêu cầu 1 | 100% |
| 2 | Yêu cầu 4 | 100% |
| 3 | Yêu cầu 7 | 100% |
| 4 |  |  |
| 5 |  |  |

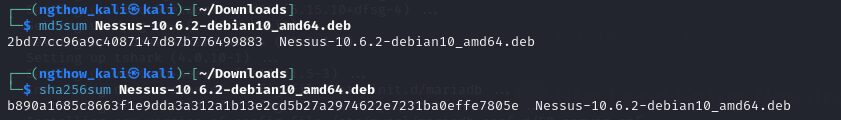
**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

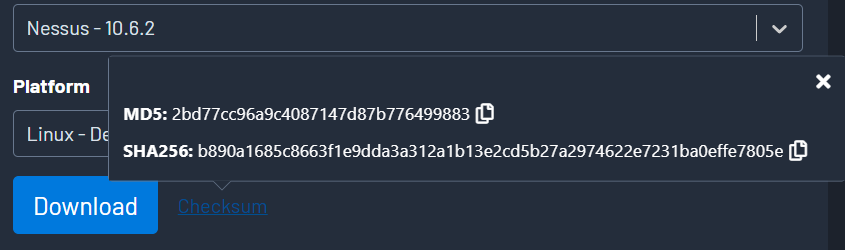
## Kịch bản 01: Quét lỗ hổng sử dụng công cụ Nessus:

1. **Cài đặt Nessus:**

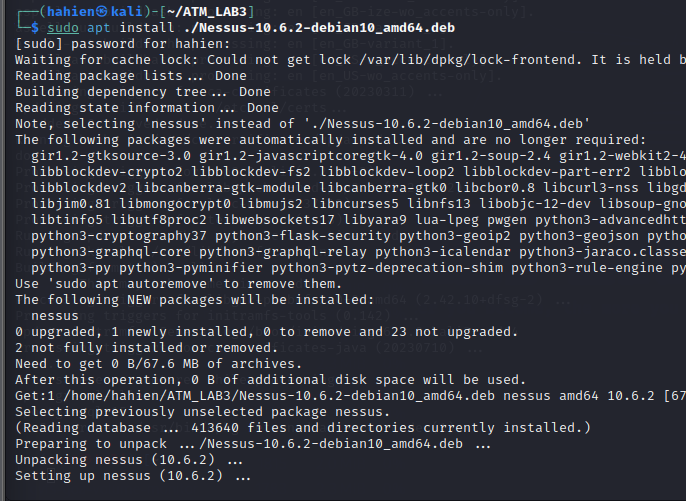
* Kiểm tra checksum của file vừa tải:



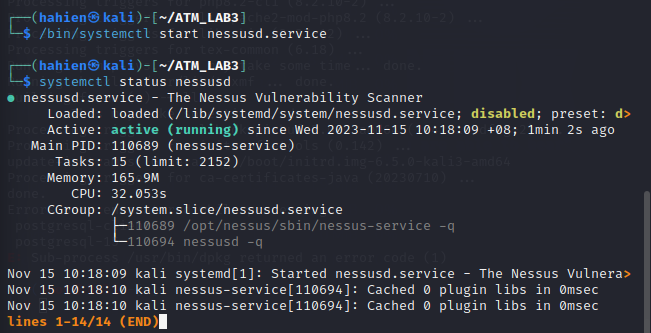
So với checksum trên web, nhận thấy đã trùng khớp:



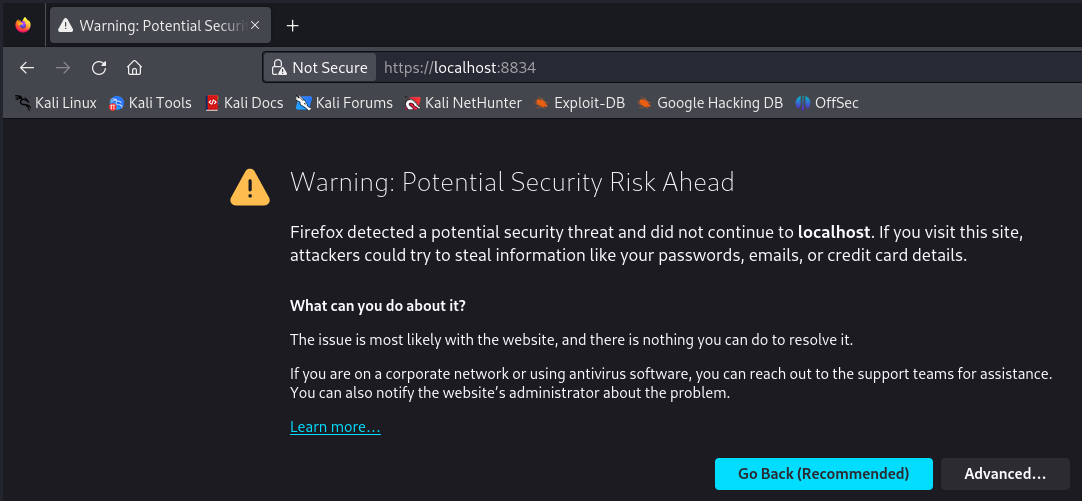
* Sau khi đảm bảo tính toàn vẹn được bảo toàn trong quá trình tải tập tin về máy, thực hiện cài đặt bằng lệnh **apt**:

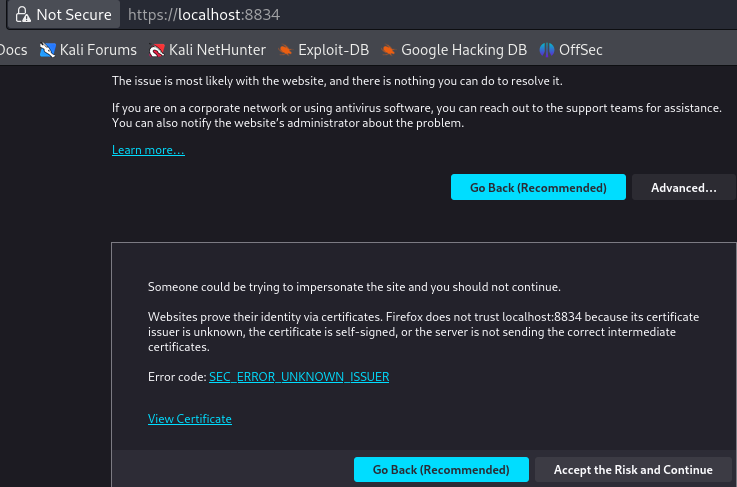


* Sau khi cài đặt thành công, thực hiện khởi động dịch vụ nessusd:

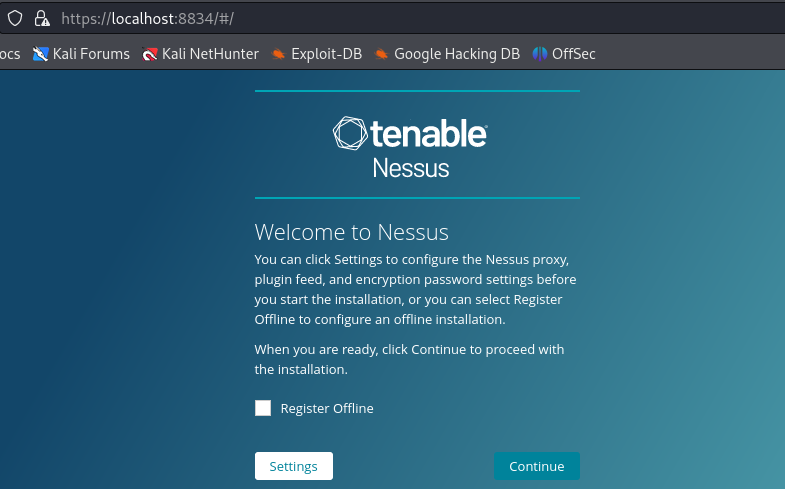


* Sau khi khởi động Nessus, mở trình duyệt và truy cập vào đường dẫn <https://localhost:8834/> :

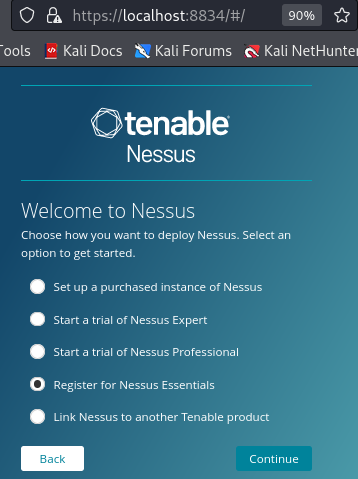




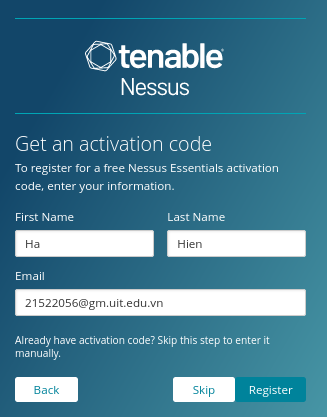
* Đã mở được trang Nessus:



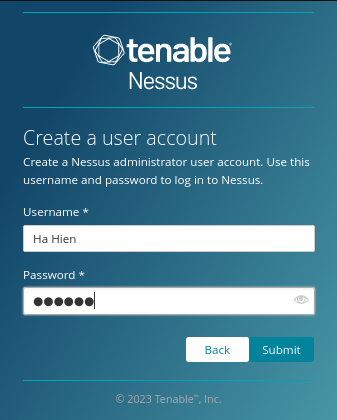
* Sau khi trang được tải lên, chúng ta được thông báo chọn phiên bản Nessus muốn sử dụng. Trong trường hợp này, chọn *Nessus Essentials*, sau đó chọn *Continue*:



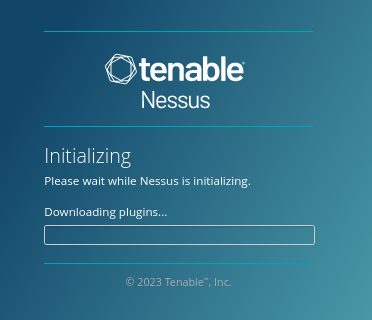
* Tiếp theo, nhập các thông tin theo yêu cầu:

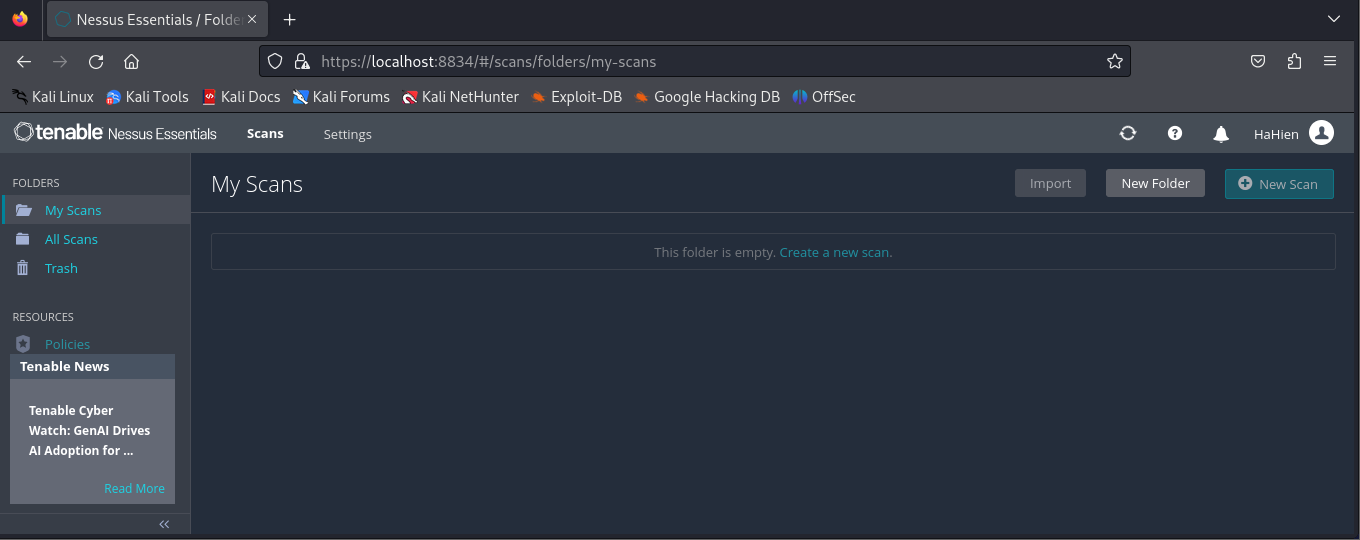


* Tạo tài khoản quản trị Nessus. Nhập tên username, password và sau đó nhấn *Submit*:



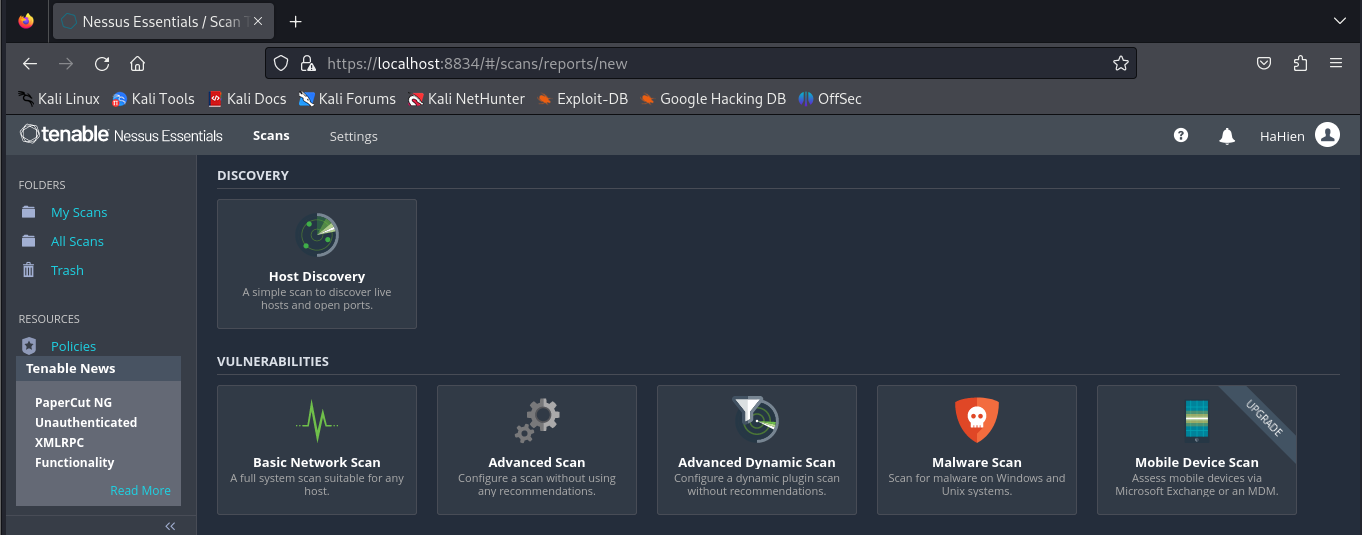
* Cuối cùng, chờ quá trình cập nhật và cài đặt các plugin hoàn tất. Quá trình này sẽ mất khá nhiều thời gian:



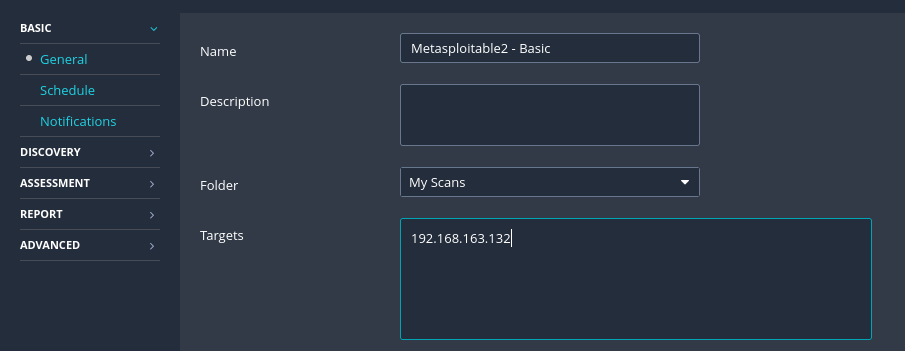


1. **Khai báo đối tượng:**

* Sau khi Nessus được cài đặt thành công, thực hiện scan lần đầu tiên.
* Thực hiện **Basic Network Scan**:



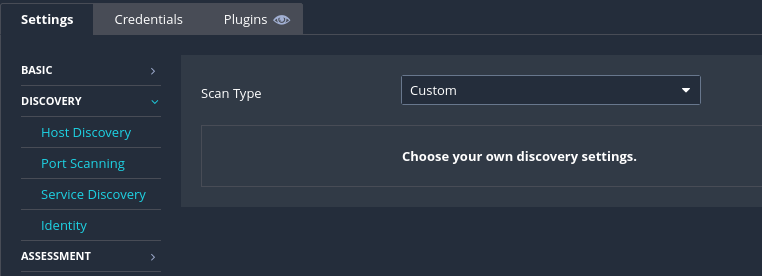
* Nhập “Metasploitable2 – Basic” trong trường *Name* và địa chỉ IP trong trường *Targets*:



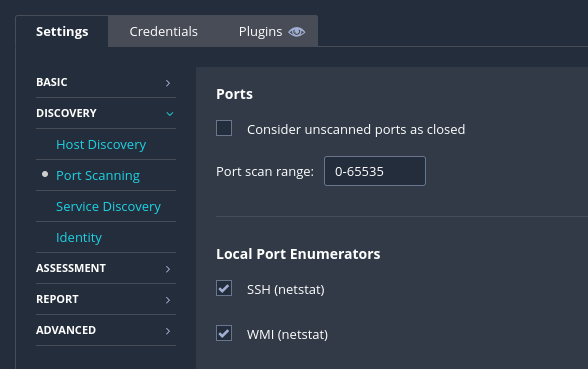
**c. Cấu hình các định nghĩa quét (Scan Definitions):**

- Mặc định, template **Basic Network Scan** chỉ thực hiện quét các port thông dụng. Tuy nhiên, bây giờ chúng ta cần thực hiện quét tất cả các port. Để thay đổi, click vào *Discovery* phía bên trái của thẻ *Settings*:

- Trong mục *Scan Type*, thay đổi giá trị từ *Port scan (common ports)* thành *Custom*:



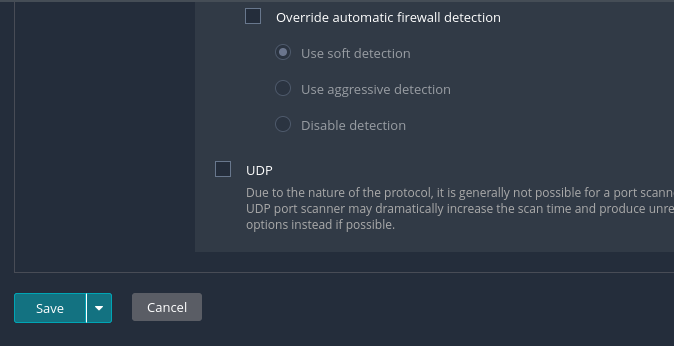
* Trong mục Port Scanning, chúng ta sẽ thiết lập dãy port muốn scan ở trong phần Port scan range. Nhập giá trị “0-65535” để thực hiện quét tất cả các port:



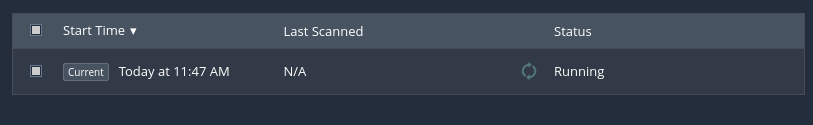
**d. Quét lỗ hổng không sử dụng tài khoản chứng thực:**

**Yêu cầu 1: Thực hiện lại các bước để quét máy Metasploitable 2 không sử dụng tài khoản chứng thực.**

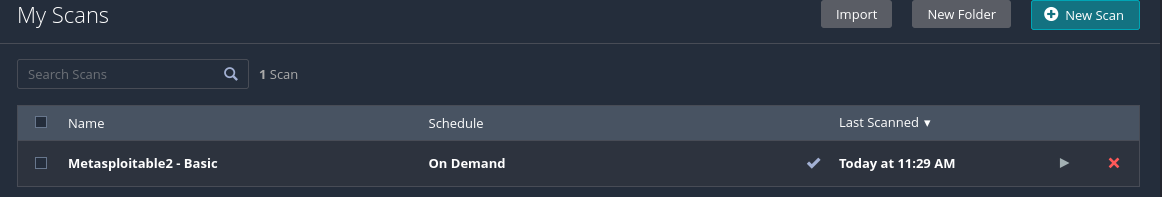
- Sau khi thiết lập mọi tham số, kéo xuống dưới và chọn *Save*:

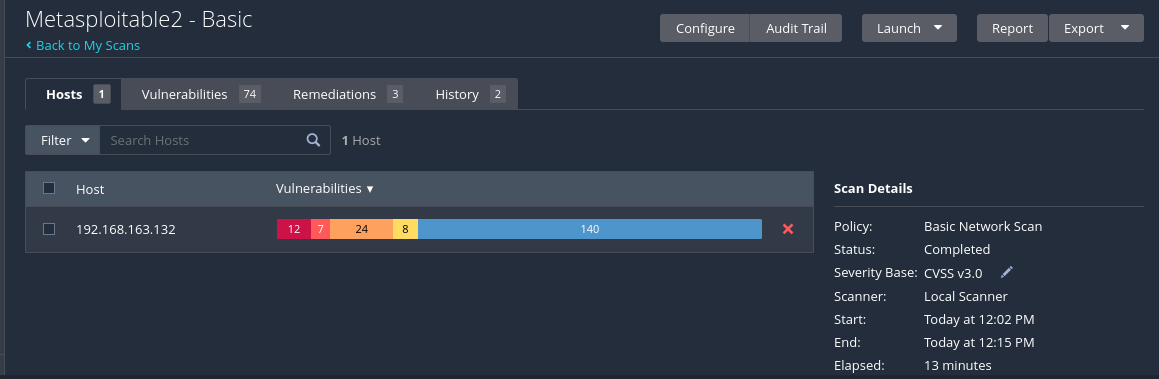


* Sau khi save, quay về mục *My Scans*, chọn vào template “*Metasploitable2 – Basic*”, sau đó chọn *Launch*. Trạng thái hiện tại được cập nhật thành *Running*:



* Sau khi quét hoàn tất, trạng thái sẽ chuyển sang *Completed*:

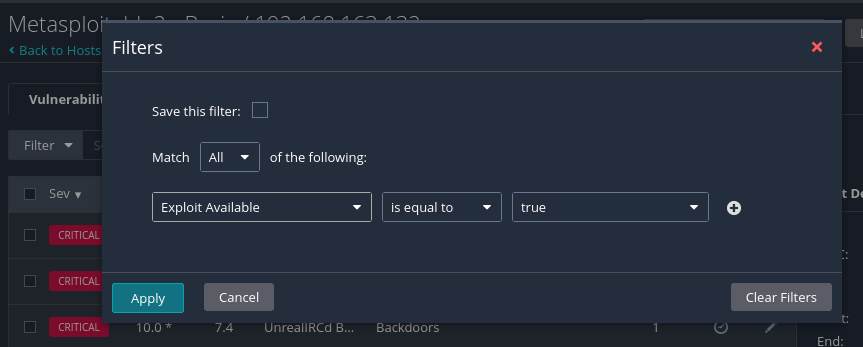




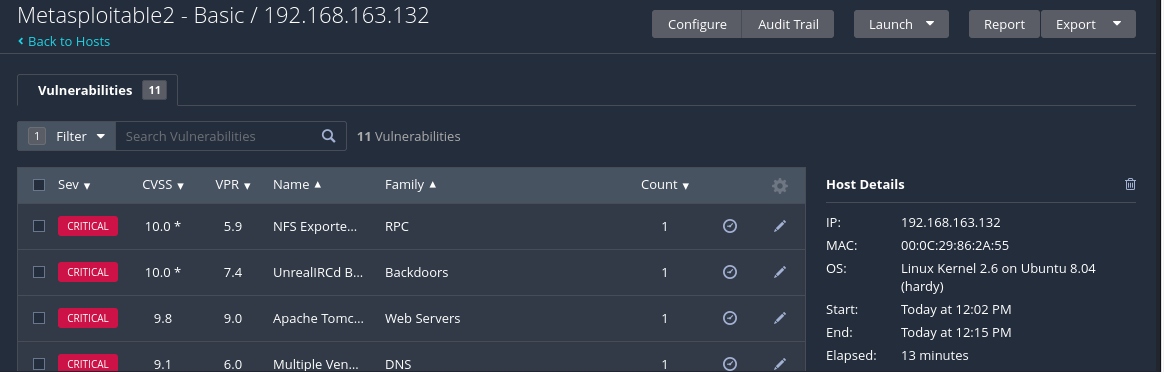
* Sau khi scan hoàn tất, click vào tên scan, *“Metasploitable2 – Basic”* để hiển thị danh sách các host được khám phá trong quá trình scan và tóm tắt các lỗ hổng tồn tại:



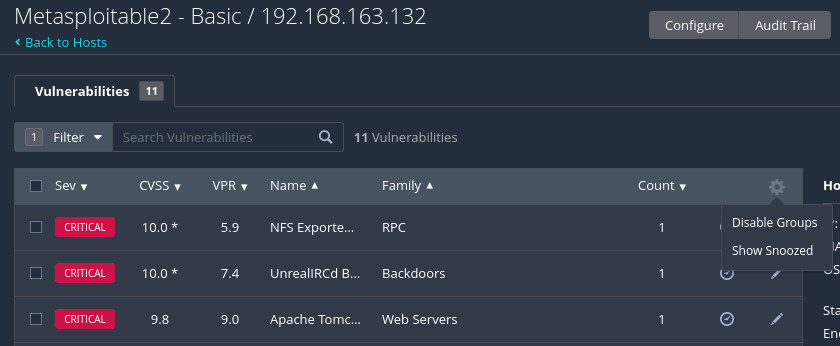
* Để hiển thị các lỗ hổng có thể dẫn đến kiểm soát máy chủ mục tiêu, chúng ta có thể click *Filter* và thay đổi giá trị lọc thành “*Exploit Available*”, giữ nguyên các giá trị mặc định của “*is equal to*” và *“true”*. Sau khi cấu hình xong, click vào *Apply*:



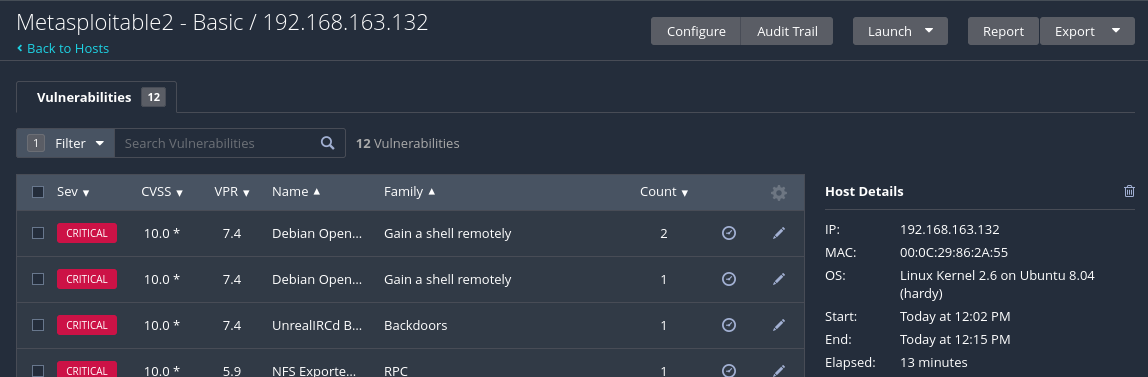
* Kết quả lọc sẽ chỉ hiển thị các lỗ hổng theo nhóm được định nghĩa bởi Nessus:



* Trong khi việc gom nhóm có thể hữu ích, chúng ta sẽ click vào biểu tượng hình bánh răng bên góc phải của bảng và chọn *Disable Groups*:



* Kết quả sẽ hiển thị danh sách tất cả lỗ hổng trên 1 trang, được sắp xếp theo mức độ ảnh hưởng:

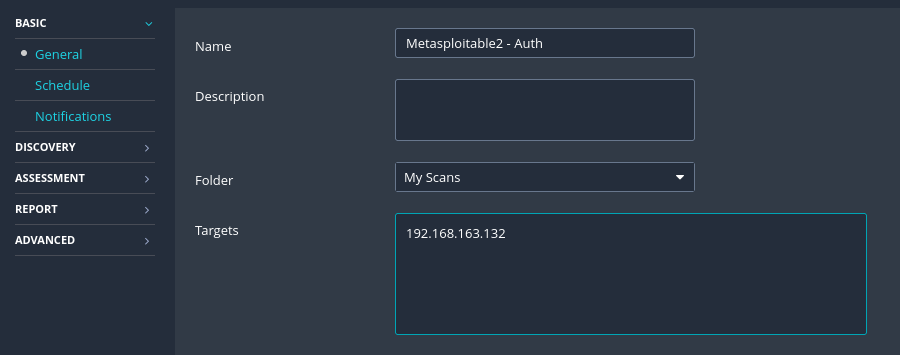


**e. Quét lỗ hổng sử dụng tài khoản chứng thực:**

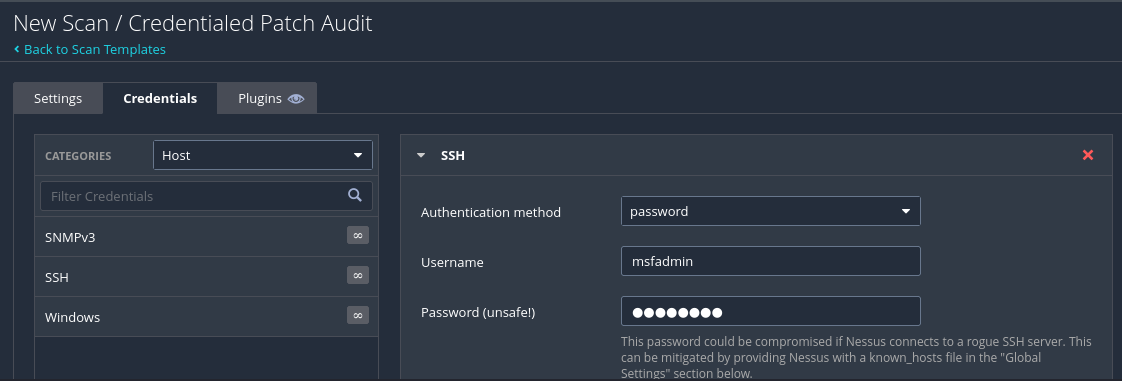
**Yêu cầu 4: Thực hiện lại các bước trên để quét máy Metasploitable 2 có sử dụng tài khoản chứng thực.**

- Chúng ta sẽ sử dụng template *Credentialed Patch Audit*, được cấu hình sẵn để thực hiện kiểm tra bảo mật cục bộ đối với máy mục tiêu:

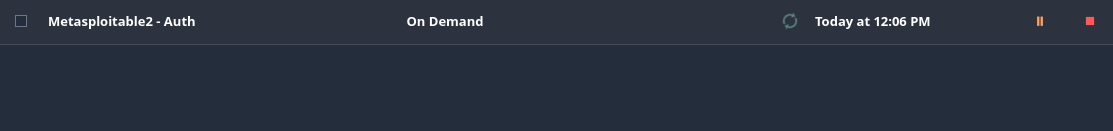
- Tương tự như *Basic Network Scan*, chúng ta cần cung cấp tên và mục tiêu cần quét:



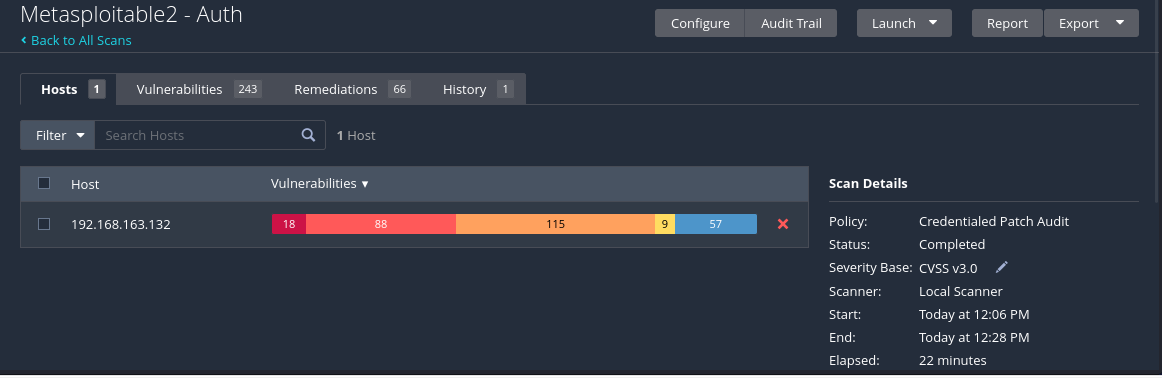
- Tiếp theo, chọn thẻ *Credentials* và chọn loại *SSH*. Trong mục *Authentication method*, chọn *password*, thiết lập username là “msfadmin” và password là “msfadmin”:

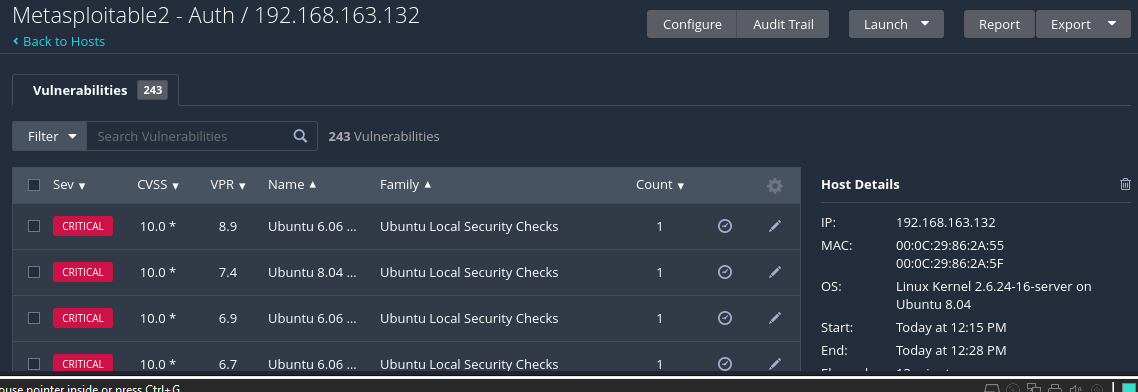


- Cuối cùng, thực hiện quét máy mục tiêu bằng cách chọn *Launch*:



- Sau khi scan chuyển sang trạng thái “Completed”, chúng ta có thể click vào tên scan và mở danh sách các host và click vào địa chỉ IP của máy metasploitable 2, kết quả sẽ hiển thị danh sách các lỗ hổng được khám phá có thể được khai thác trên máy chủ:

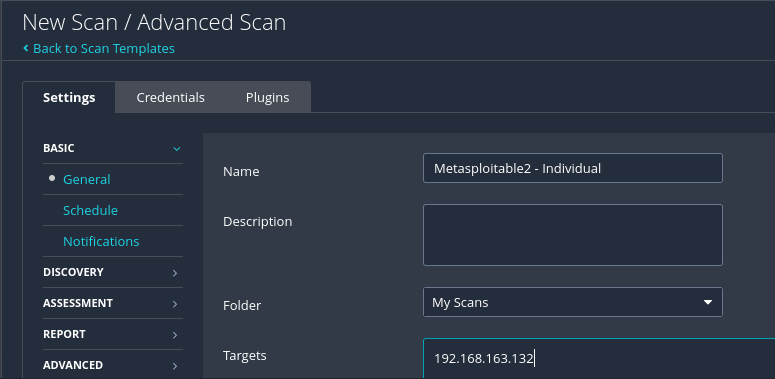




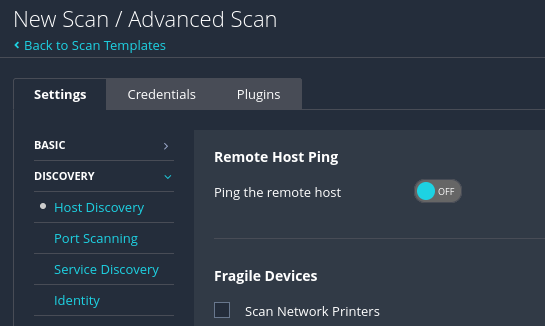
**f. Quét với Plugin được chỉ định**

**Yêu cầu 7: Thực hiện lại các bước trên để quét máy Metasploitable 2 sử dụng plugin NFS Exported Share Information Disclosure**

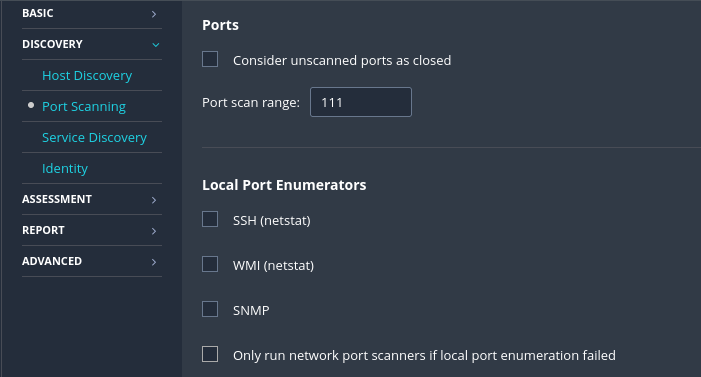
* Trong trường hợp này, chúng ta sẽ chạy plugin NFS Exported Share Information Disclosure. Để chạy scan cho một plugin, chúng ta lại bắt đầu bằng New Scan:
* Chúng ta sẽ sử dụng template Advanced Scan:
* Tương tự, cũng đặt tên và đối tượng cần scan:



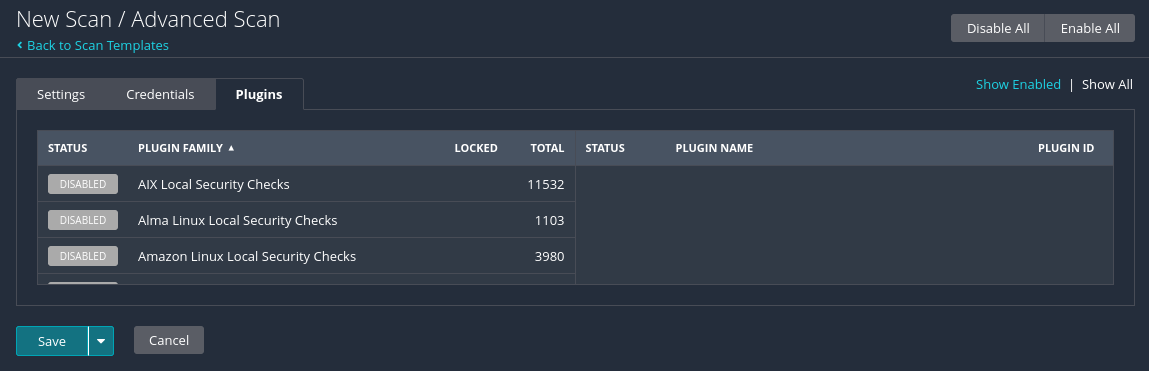
* Để tiết kiệm thời gian và ít để lại dấu vết, chúng ta sẽ tắt Host discovery, vì chúng ta biết được host vẫn còn hoạt động:



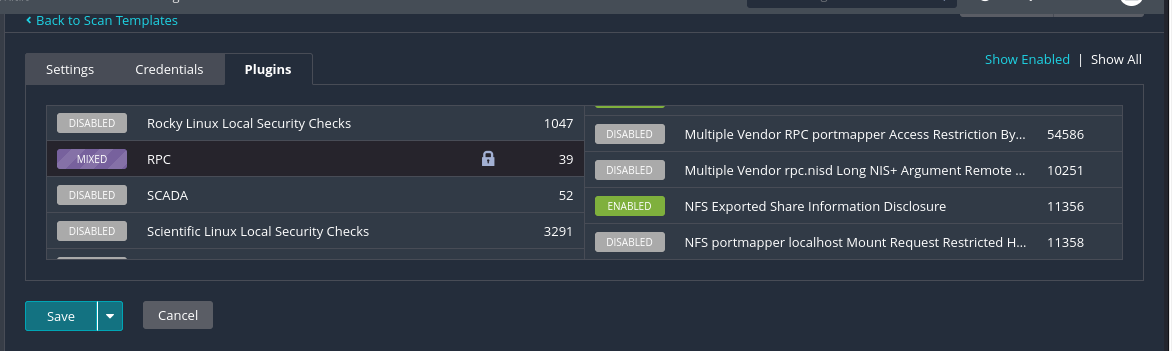
* Vì chúng ta chỉ scan dịch vụ RPC và biết rằng RPC chạy trên TCP port 111, nên chúng ta chỉ scan duy nhất port này:



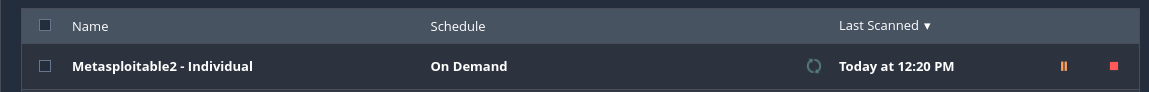
* Sau khi giảm thiếu tối đa các tùy chọn scan, bây giờ tiến hành chọn plugin. Chọn thẻ Plugins và click vào Disable All ở góc phải:



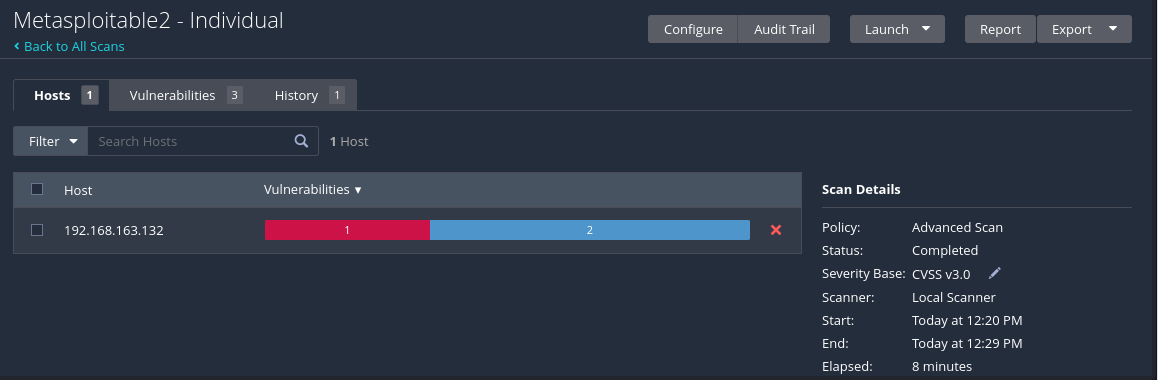
* Để tiến hành quét NFS shares, chúng ta sẽ di chuyển đến “RPC” bên cột bên trái và thiết lập “NFS Exported Share Information Disclosure” ở cột bên phải thành Enabled:

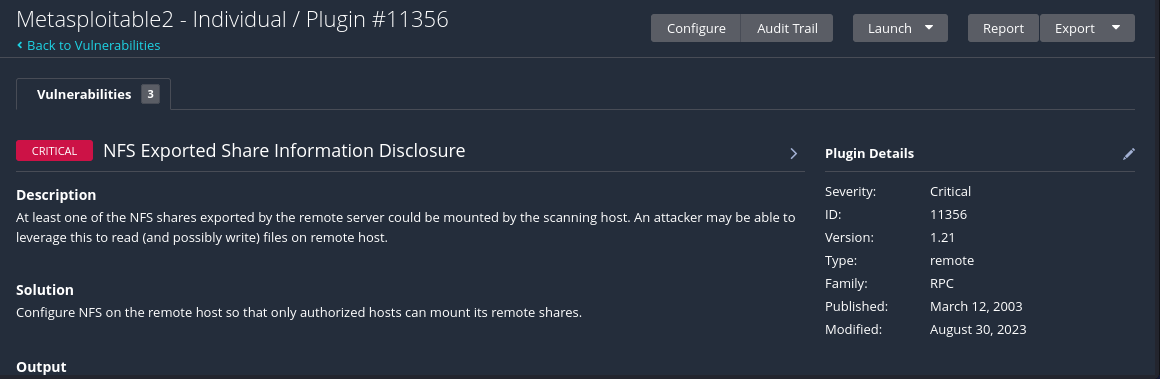


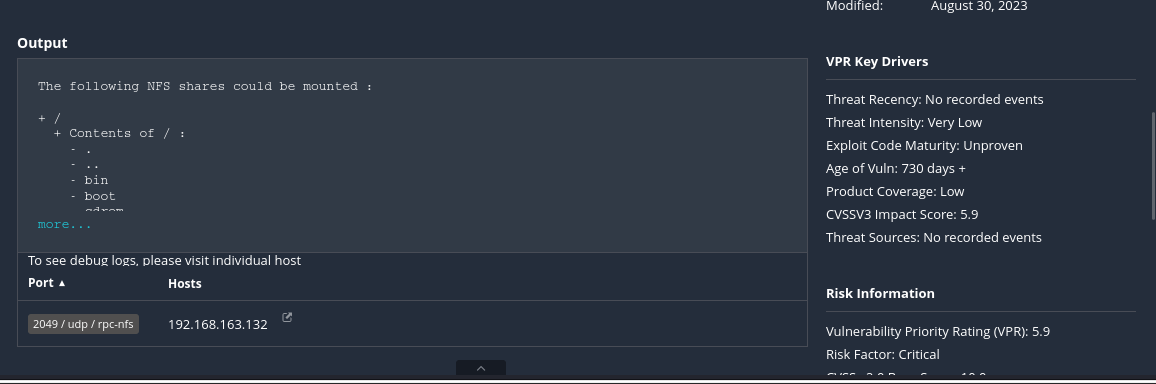
* Bây giờ ta đã cấu hình xong, tiến hành quét. Click vào Launch:



* Sau khi trạng thái quét chuyển sang “Completed”, chúng ta có thể click vào tên scan, sau đó địa chỉ IP máy mục tiêu. Di chuyển đến lỗ hổng Critical duy nhất và click vào để hiển thị chi tiết thông tin lỗ hổng:







---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **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 .DOCX và .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 đã đăng ký với GVHD-TH).

*Ví dụ: [*NT101.K11.ATCL*]-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 bài Lab.
* 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 được bài thực hành. Khuyến khích:

* Chuẩn bị tốt.
* Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

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

**HẾT**

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