Cyber Operations

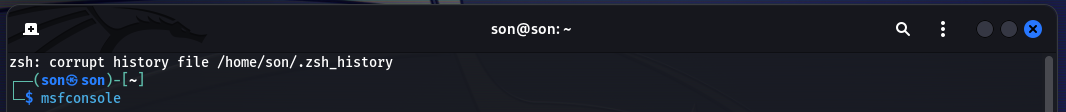
Unit 08 – Metasploit and Armitage

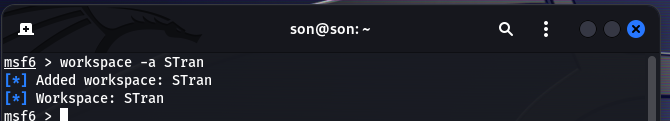
# **Lab 06 – Metasploit and Vulnerabilities**

### **MEtasploit Workspaces**

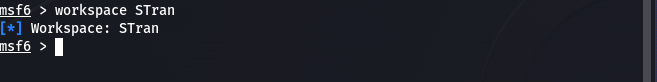
Add a workspace to your Metasploit database with the format of first\_initial+last\_name, then, switch to the workspace you just created.

Take a screenshot showing that your newely created workspace is selected.









### **Importing into Metasploit**

Log into Nessus and export the scan data you gathered in the previous lab to the .nessus format. Export you OpenVAS scan data you generated in the previous lab to an XML file as well. From your nmap vulnerability scan, you should already have an XML file of your results. Import these three scans into Metasploit, and take a screenshot of the results of the hosts command within Metasploit.

1. Đăng nhập vào Nessus:

* Mở trình duyệt web và truy cập vào giao diện Nessus.
* Sử dụng thông tin đăng nhập của bạn để đăng nhập vào tài khoản Nessus.

1. Xuất dữ liệu quét từ Nessus sang định dạng .nessus:

* Trong giao diện Nessus, điều hướng đến phần kết quả quét hoặc báo cáo quét.
* Tìm và chọn quét mà bạn đã thực hiện trước đó.
* Tìm tùy chọn xuất dữ liệu hoặc tải xuống.
* Chọn định dạng .nessus và lưu tệp xuống máy tính của bạn.

1. Xuất dữ liệu quét từ OpenVAS sang tệp XML:

* Trong giao diện OpenVAS, điều hướng đến phần kết quả quét hoặc báo cáo quét.
* Chọn quét mà bạn đã thực hiện trước đó.
* Tìm tùy chọn xuất dữ liệu hoặc tải xuống.
* Chọn định dạng XML và lưu tệp xuống máy tính của bạn.

1. Xuất dữ liệu quét từ nmap sang tệp XML:

* Tìm tệp XML kết quả quét từ nmap mà bạn đã tạo ra trong lab trước.
* Sao chép hoặc di chuyển tệp XML này vào máy tính của bạn.

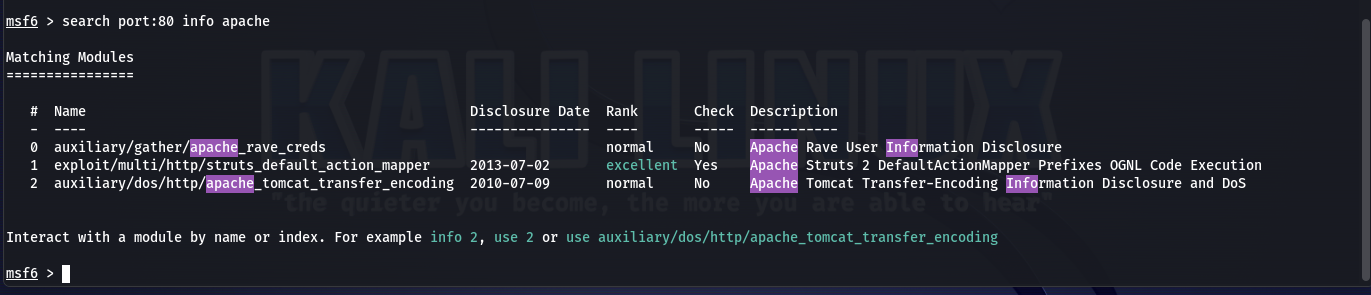
1. Nhập ba quét này vào Metasploit:

* Mở Metasploit và đăng nhập vào giao diện.
* Tìm tùy chọn để nhập dữ liệu quét hoặc kết quả quét từ các công cụ khác nhau.
* Chọn các tệp .nessus, XML tương ứng và nhập chúng vào Metasploit.

### **Using the Database**

Search the database for the following in a single command:

* Show the port and info columns
* Search only for port 80
* Limit the results with the search string Apache.



Take a screenshot of the command you used to find them in a single screenshot.

Manually add the credentials found into the database, as credentials found with some scans don’t always import properly.

After you have added the credentials, run the creds command and take a screenshot.

From the results of your scans, you should know about some highly exploitable services and hosts. Find a module to take advantage of one of these services. Once you have the module, select it, and set up the options for it. After entering the options, type show options and take a screenshot.