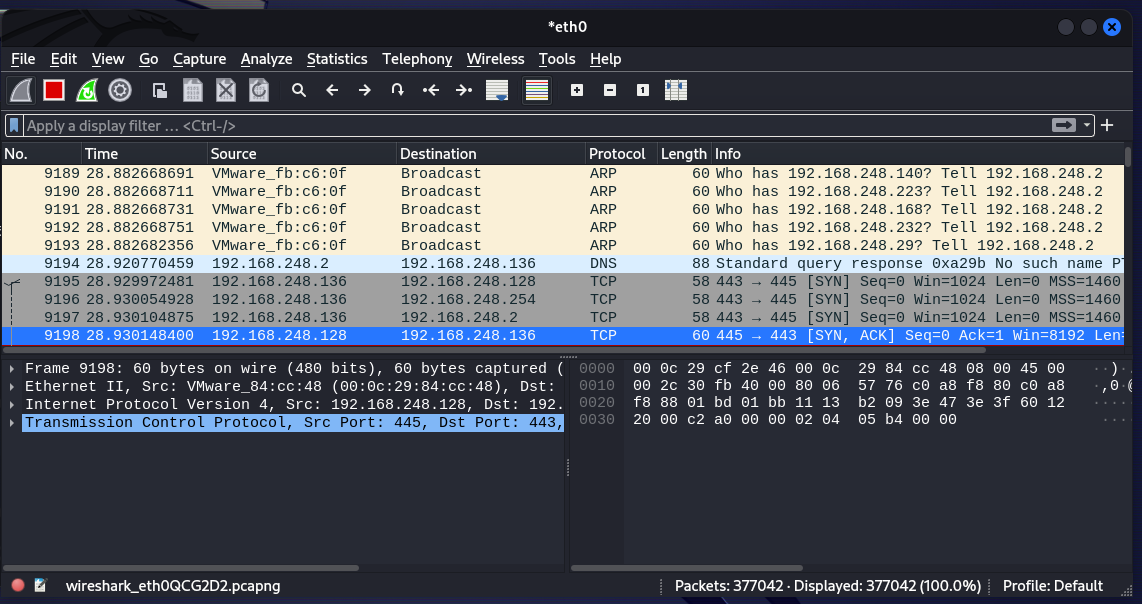
### **Advanced Port Scanning with Nmap**

On your Kali machine, start a Wireshark packet capture. While the capture is running, start a port scan with the following parameters:

* Scan type: Syn Scan
* Timing: T4
* Source Port:443
* Range: 192.168.1.0/24 (Or your internal network range)

Once that scan finishes, stop your Wireshark capture. Finding multiple packets coming from your host to the destination with a source port of 443 and the target destination port of whatever nmap was checking. Take a screenshot that shows that your scans were coming from port 443 in Wireshark.

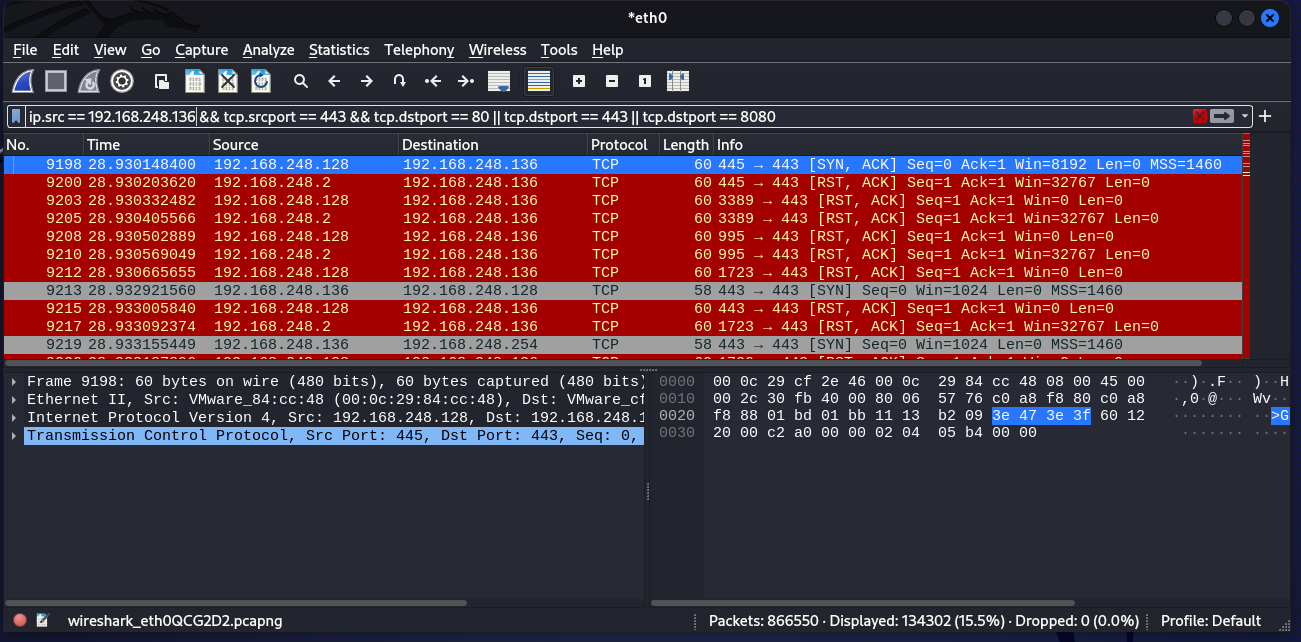
Mở Wireshrark và bắt đầu quét

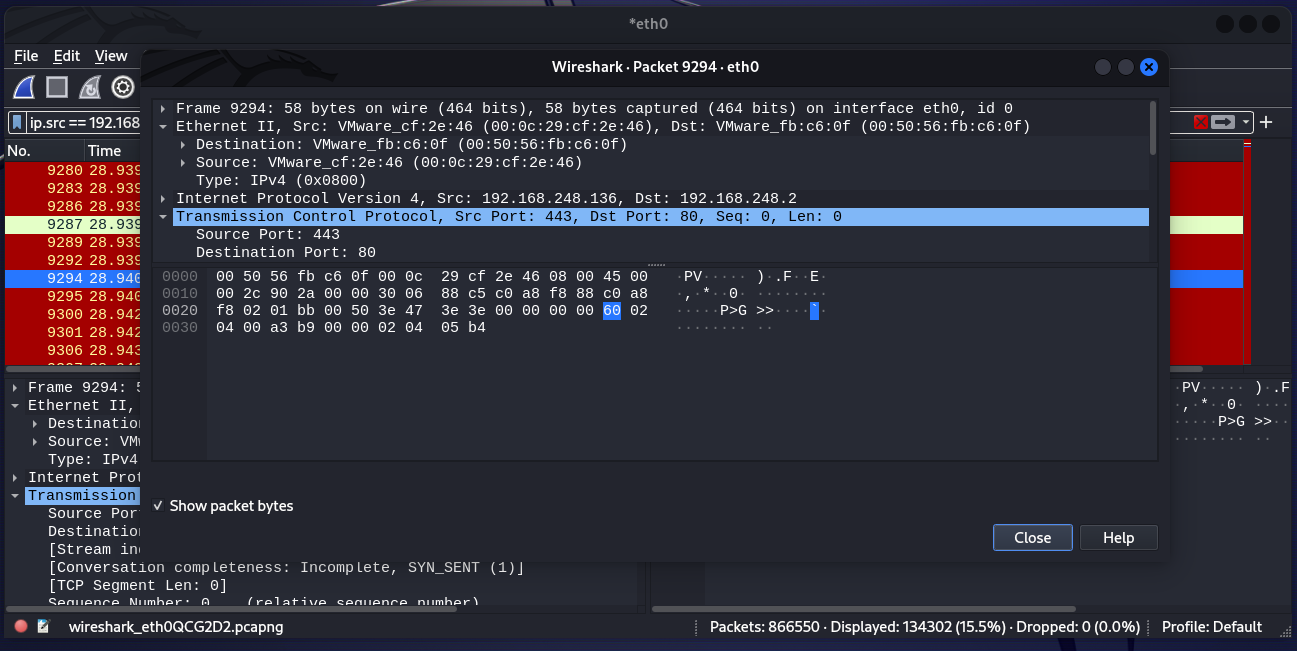


Thực hiện quét cổng, chạy lệnh sau trong một cửa sổ Terminal mới:



Khi quét cổng hoàn thành, quay lại cửa sổ Wireshark và nhấn nút "Stop" hoặc nhấn tổ hợp phím Ctrl + E để dừng việc bắt gói tin. => Trong giao diện Wireshark, sử dụng bộ lọc để tìm các gói tin có nguồn từ máy bạn (host) và có cổng nguồn là 443 và cổng đích là các cổng mà Nmap đã kiểm tra.

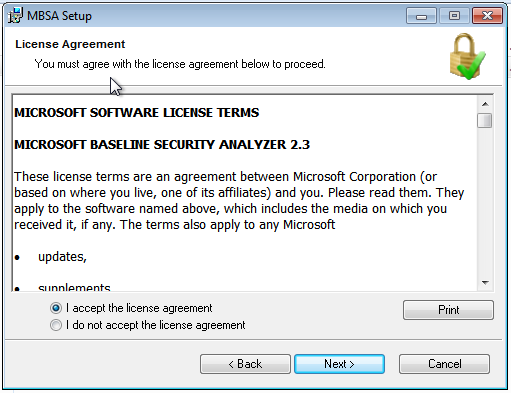


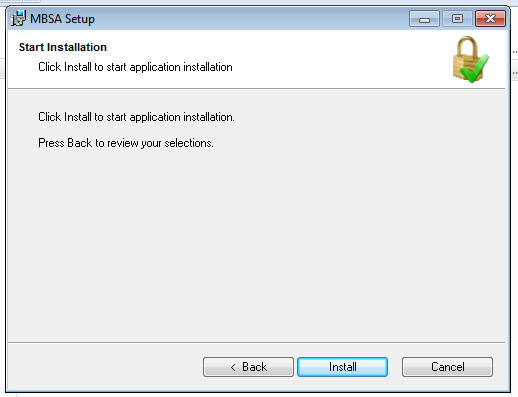


### **MBSA**

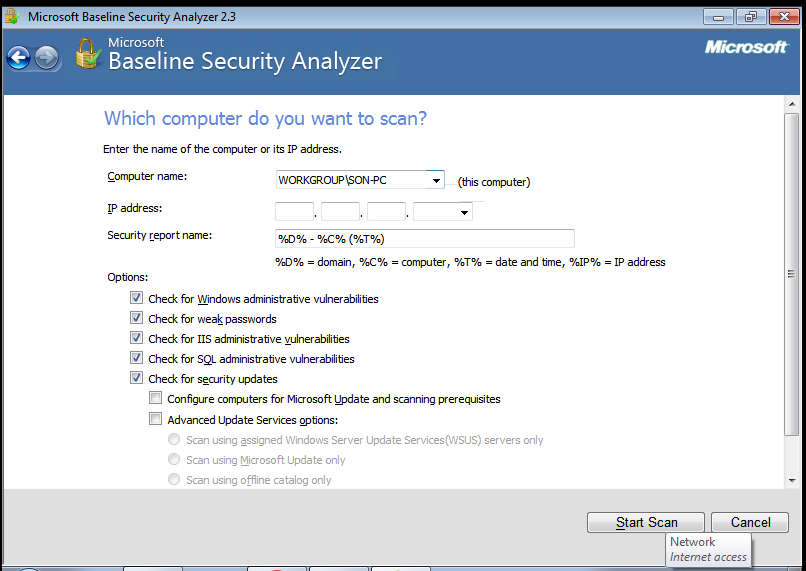
Install the MBSA tool from Microsoft on a Windows host. Perform a scan against your local machine that you installed MBSA on. Take a screenshot of the finalized results.

Cài đặt MBSA

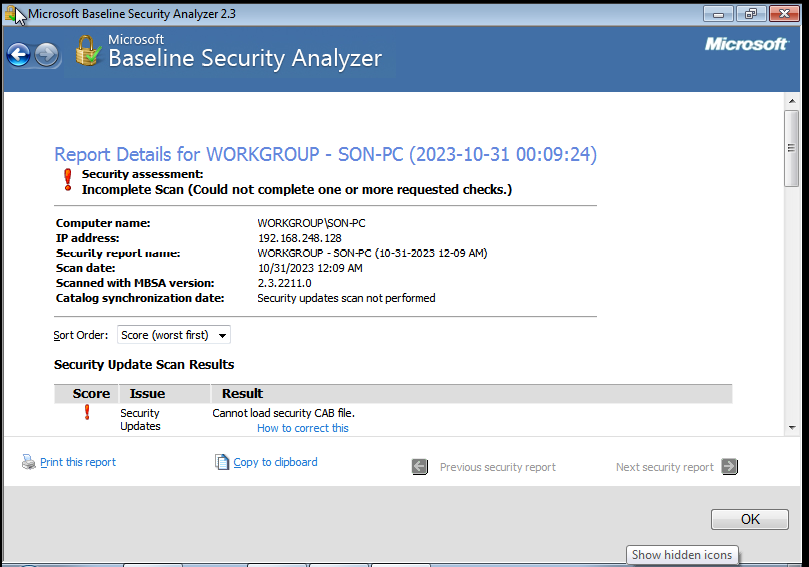
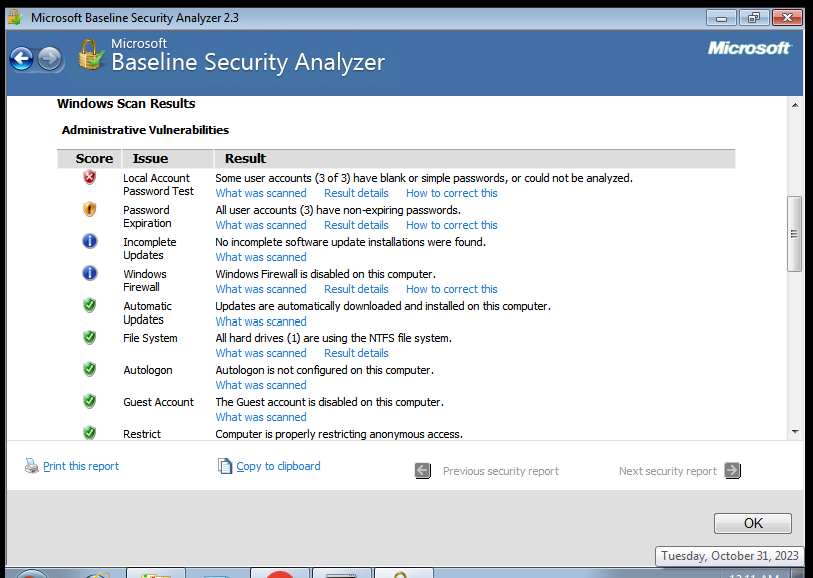


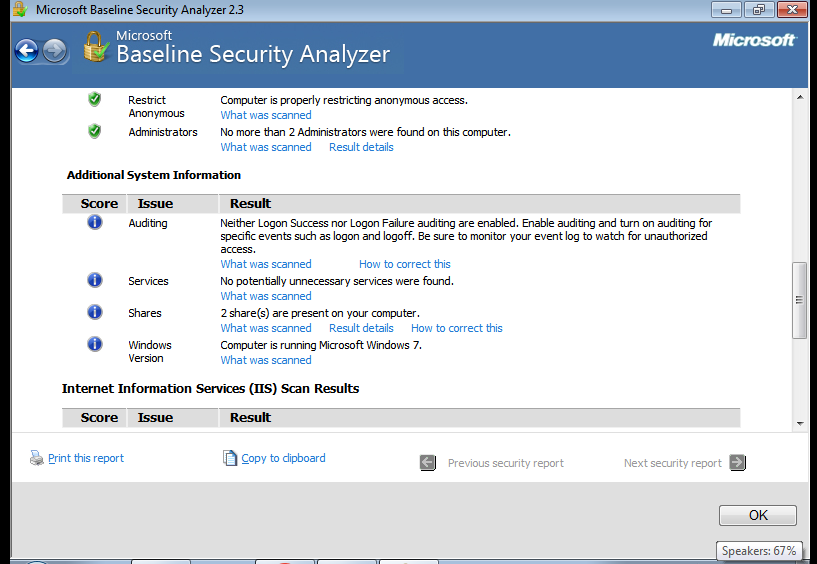


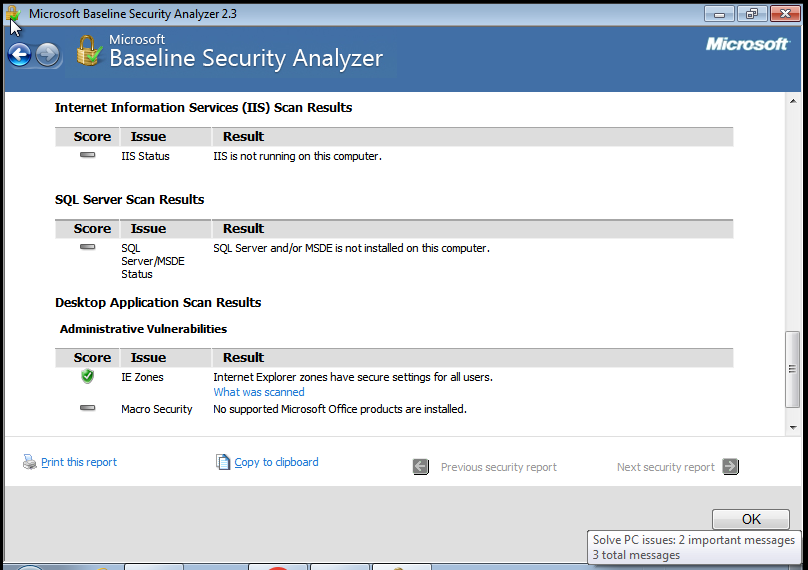
Click Start Scan để bắt đầu scan



Đây là kết quả sau khi scan







### **Nessus**

Register for and install Nessus home on your Kali VM. Configure a custom scan policy based off the Basic Network Scan policy that Nessus comes with. The scan policy should contain your name. When creating the scan, upload your fping.txt file from the previous labs so that all hosts are scanned in the network (excluding Kali), or manually type in the hosts. Launch the scan with Nessus and take a screenshot of the hosts summary once the scan completes.

* Truy cập trang web của Tenable và đăng ký tài khoản để nhận giấy phép Nessus Home.
* Sau khi có giấy phép, tải xuống phiên bản Nessus Home cho Kali Linux từ trang web của Tenable.
* Mở terminal trên Kali VM và di chuyển đến thư mục chứa tệp tin Nessus Home.
* Sử dụng lệnh sau để cài đặt Nessus Home trên Kali:
* *sudo dpkg -i <tên\_tệp\_tin.deb>* (Thay thế `<tên\_tệp\_tin.deb>` bằng tên thực tế của tệp tin Nessus Home bạn đã tải xuống)
* Khi quá trình cài đặt hoàn tất, chạy lệnh sau để khởi động dịch vụ Nessus: *sudo systemctl start nessusd*
* Truy cập vào giao diện web của Nessus bằng cách mở trình duyệt và nhập địa chỉ: https://localhost:8834.
* Trong trình duyệt, bạn sẽ được yêu cầu chấp nhận các điều khoản và tạo một người dùng quản trị cho Nessus. Làm theo hướng dẫn để hoàn thành quá trình cài đặt.
* Trong giao diện web Nessus, chọn "Scans" (Quét) từ thanh điều hướng bên trái.
* Nhấp vào nút "New Scan" (Quét mới) để tạo một quét mới.
* Đặt tên cho quét và chọn chính sách quét tùy chỉnh mà bạn đã tạo trong bước trước.
* Để quét các máy chủ trong mạng (ngoại trừ Kali Linux) từ tệp fping.txt, chọn "Import targets from file" (Nhập mục tiêu từ tệp tin) và tải lên tệp fping.txt đã được tạo trong các lab trước, hoặc nhập thủ công các máy chủ cần quét.
* Tiếp theo, điều chỉnh các thiết lập khác (nếu cần) và nhấp vào nút "Save" (Lưu) để tạo quét.
* Trên trang quản lý quét, nhấp vào tên quét mà bạn đã tạo để mở chi tiết.
* Nhấp vào nút "Launch" (Khởi chạy) để bắt đầu quét.
* Chờ quá trình quét hoàn thành.
* Sau khi quét hoàn thành, chọn "Hosts" (Máy chủ) từ thanh điều hướng bêntrái để xem tóm tắt các máy chủ đã được quét.

### **OpenVAS**

Startup OpenVAS in your Kali machine and create a new scan containing your name + Target (firstLast Target). The hosts of this scan should include your entire testing network. Change the Alive Test to **ICMP, TCP-ACK Service & ARP Ping**. Once you have that scan target defined, create a new scan task with your name + Scan. Set the target of this scan to the target we created in the previous step, change the Scan config to **Full and fast ultimate**, and set the order of the targets to be **random**. Run the scan and allow it to complete, then, click on the report and download a PDF copy of it. Open up that PDF and take a screenshot of the Results Overview section.

* Mở terminal trên Kali Linux.
* Chạy lệnh sau để khởi động OpenVAS: *sudo openvas-start*
* Trong terminal, chạy lệnh sau để mở giao diện web của OpenVAS:
* *sudo openvas-stop*
* *sudo openvas-start*
* *sudo openvas-setup*
* *sudo openvas-start*
* *sudo openvas-check-setup*
* *sudo openvas-stop*
* *sudo greenbone-nvt-sync*
* *sudo openvas-start*
* *sudo openvasmd --rebuild --progress*
* *sudo openvasmd --update --progress*
* *sudo openvasmd --migrate --progress*
* *sudo openvasmd --rebuild --progress*
* *sudo openvas-start*
* (Lưu ý: Các lệnh trên sẽ tạo ra và cấu hình OpenVAS cho lần chạy đầu tiên)
* Mở trình duyệt và truy cập vào giao diện web của OpenVAS bằng cách nhập địa chỉ sau: https://localhost:9392.
* Đăng nhập vào giao diện web bằng tài khoản quản trị đã tạo trong quá trình cài đặt.
* Trong giao diện web OpenVAS, chọn "Scans" (Quét) từ thanh điều hướng bên trái.
* Nhấp vào nút "Create Scan" (Tạo quét) để tạo một quét mới.
* Đặt tên cho quét bằng cách kết hợp tên của bạn và tên mục tiêu (ví dụ: "firstLast Target").
* Trong phần "Targets" (Mục tiêu), nhập địa chỉ mạng hoặc danh sách các máy chủ mà bạn muốn quét.
* Trong phần "Alive Test" (Kiểm tra trạng thái sống), chọn các tùy chọn "ICMP", "TCP-ACK Service", và "ARP Ping".
* Điều chỉnh các thiết lập khác (nếu cần) và nhấp vào nút "Save" (Lưu) để tạo quét.
* Sau khi tạo quét, quay lại trang quản lý quét và chọn quét mà bạn đã tạo.
* Nhấp vào nút "Create Task" (Tạo nhiệm vụ) để tạo một nhiệm vụ quét mới.
* Đặt tên cho nhiệm vụ quét bằng cách kết hợp tên của bạn và "Scan" (ví dụ: "firstLast Scan").
* Trong phần "Target" (Mục tiêu), chọn mục tiêu quét mà bạn đã tạo ở bước trước.
* Trong phần "Scan config" (Cấu hình quét), chọn cấu hình "Full and fast ultimate".
* Trong phần "Order" (Thứ tự), chọn "Random" để quét các mục tiêu theo thứ tự ngẫu nhiên.
* Nhấp vào nút "Save" (Lưu) để tạo nhiệm vụ quét.
* Trên trang quản lý nhiệm vụ quét, chọn nhiệm vụ quét mà bạn đã tạo.
* Nhấp vào nút "Play" (Chạy) để bắt đầu quá trình quét.
* Chờ quá trình quét hoàn thành.
* Khi quét đã hoàn thành, chọn nút"Reports" (Báo cáo) từ thanh điều hướng bên trái.
* Trong danh sách báo cáo, tìm báo cáo tương ứng với nhiệm vụ quét mà bạn đã chạy.
* Nhấp vào báo cáo để mở nó.
* Trên trang báo cáo, chọn nút để tải xuống bản sao PDF của báo cáo.
* Mở tệp PDF và chụp màn hình phần "Results Overview" (Tổng quan kết quả).