HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOAN AN TOÀN THÔNG TIN

BÁO CÁO THỰC HÀNH

Bài 8: Bắt dữ liệu mạng

Họ và tên: VũThành Long

Mã sinh viên: B21DCAT012

Nhóm: 06

Môn học: Thực tập cơ sở

Giảng viên giảng dạy: Nguyễn Hoa Cương

Hà Nội, 2024

Mục lục

I. Tìm hiểu lý thuyết:

– tcpdump:

- tcpdump là một công cụ phân tích gói tin mạng chạy dưới giao diện dòng lệnh (CLI). Nó cho phép người dùng hiển thị các gói tin TCP/IP đang được truyền hoặc nhận qua mạng mà máy tính chạy tcpdump kết nối tới.
- tcpdump có mặt trên Windows và các hệ điều hành họ Unix như Linux, BSD, MacOS, OpenWRT, v.v
- Một số tác dụng của tcpdump (và các công cụ bắt gói tin nói chung) trên thực tế:
- Giám sát hạ tầng mạng để phát hiện các kết nối bất thường.
- Tấn công ăn trộm tên tài khoản, mật khẩu và các thông tin nhạy cảm khác nếu dữ liệu được truyền qua HTTP không mã hoá.
- Kiểm tra lỗi trên hạ tầng mạng (định tuyến sai, cổng đóng, v.v).
- tcpdump có thể lưu kết quả bắt gói tin vào tệp pcap.

– Wireshark:

- Wireshark là một công cụ phân tích gói tin mạng mã nguồn mở và miễn phí, được sử dụng rộng rãi trên thế giới. Wireshark có mặt trên Windows và các hệ điều hành họ Unix.
- Khác với tcpdump, Wireshark có giao diện đồ hoạ (GUI) giúp người dùng dễ tương tác hơn.
- Wireshark khá giống với tcpdump. Một số tính năng của Wireshark liệt kê dưới đây cũng có mặt trên tcpdump:
- Hỗ trợ nhiều giao thức mạng khác nhau.
- Giám sát hạ tầng mạng trên thời gian thực.
- Bắt các gói tin trên thời gian thực, có thể lưu lại và kiểm tra sau.
- Hỗ trợ đọc ghi nhiều loại tệp dữ liệu: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, v.v
- Hỗ trợ phân tích VoIP.

- Có thể xuất dữ liệu dưới dạng XML, PostScript, CSV hoặc plain text.

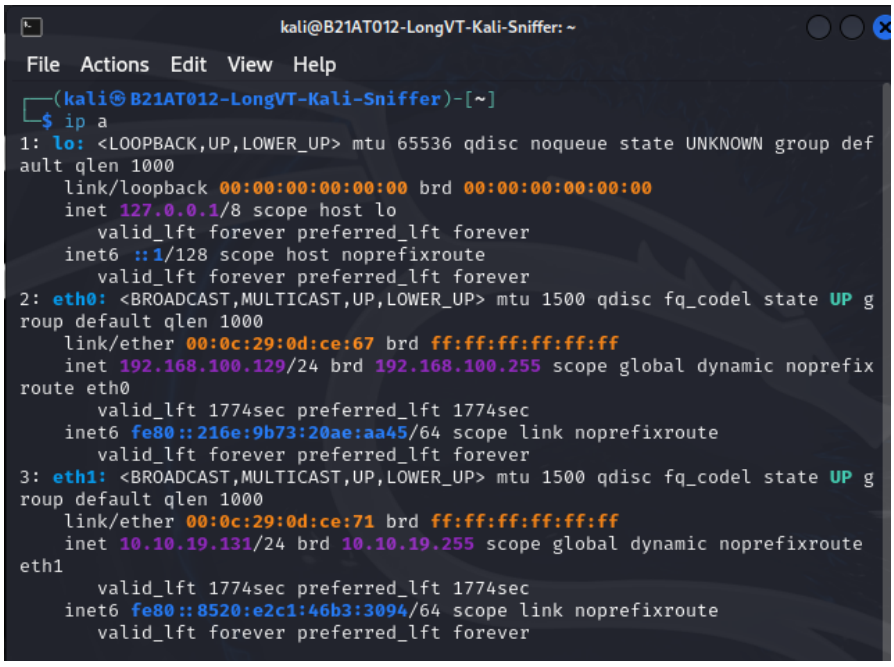
– NetworkMiner:

- NetworkMiner là một công cụ phân tích mạng (NFAT) mã nguồn mở dành cho Windows.
- Tương tự như tcpdump và Wireshark, NetworkMiner có thể được sử dụng như một công cụ bắt / dò tìm gói tin mạng thụ động để phát hiện hệ điều hành, phiên, tên máy chủ, cổng đang mở, v.v. mà không đặt bất kỳ lưu lượng nào trên mạng.
- NetworkMiner có thể lưu kết quả bắt gói tin vào tệp pcap.

II. Mô tả cài đặt & kết quả:

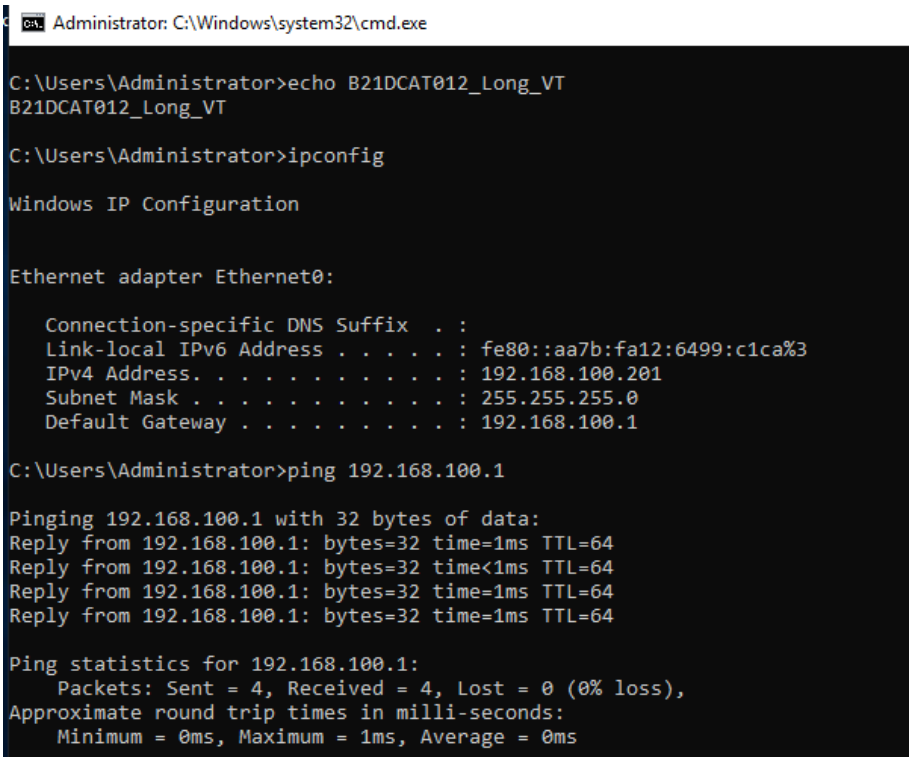
– Sử dụng tcpdump:

- Trước hết, sinh viên cấu hình Sniffer gia nhập hai mạng Internal và External. **Internal là eth0, external là eth1.**

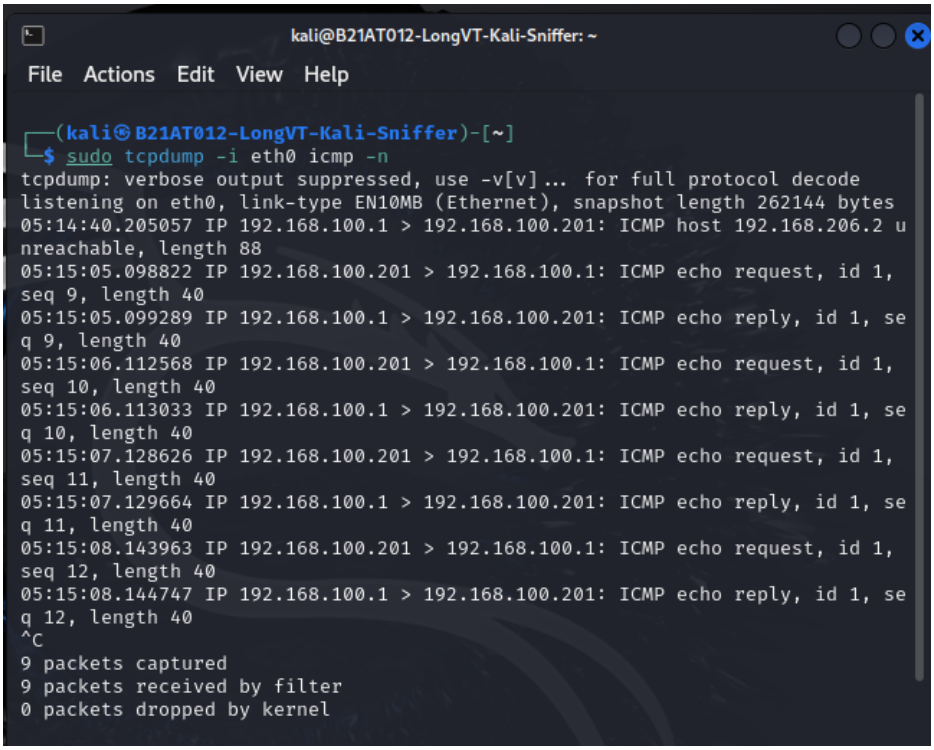


- Tiếp theo, chạy **sudo tcpdump -i eth0 icmp -n** để bắt gói tin ping trên mạng internal.

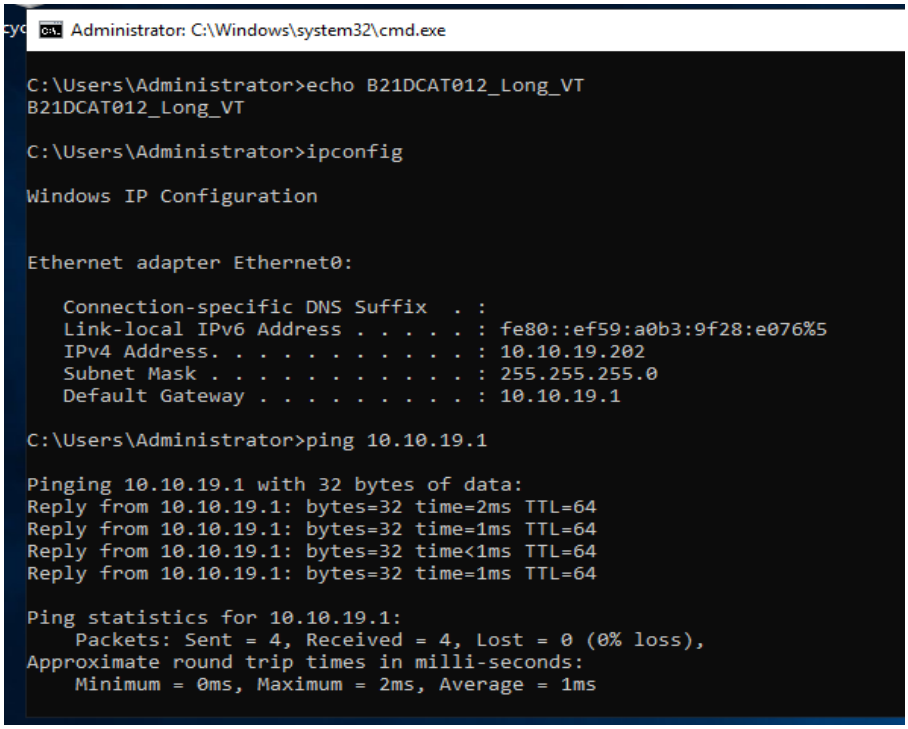
- Thực hiện ping từ Windows Server Internal đến pfSense như hình dưới.

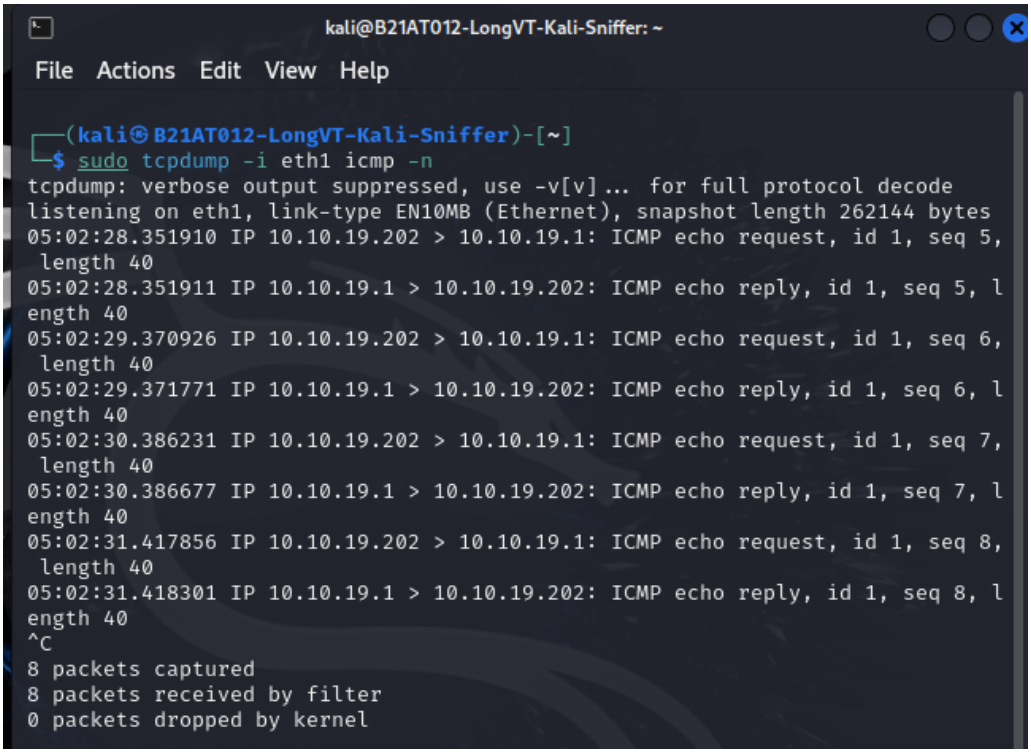


- Kết quả, tcpdump bắt được các gói tin, trong đó xen kẽ là gói tin ping gửi từ Windows Server Internal địa chỉ 192.168.100.201 đến pfSense 192.168.100.1 và gói tin trả lời từ pfSense đến Windows Server Internal.

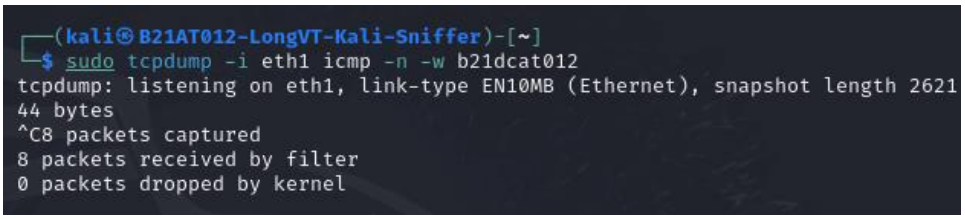


- Thực hiện tương tự với mạng External và cũng bắt được các gói tin trao đổi giữa Windows Server External 10.10.19.202 và 10.10.19.1.

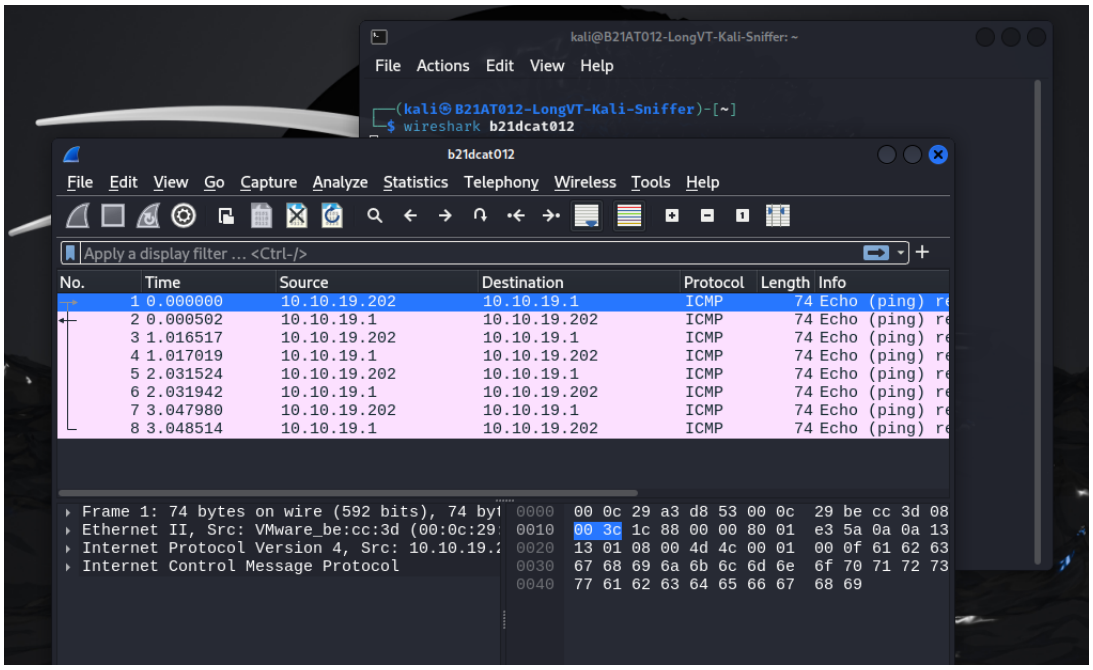




- Để lưu kết quả vào file, dùng lệnh **sudo tcpdump -i eth1 icmp -w <tênfile>**

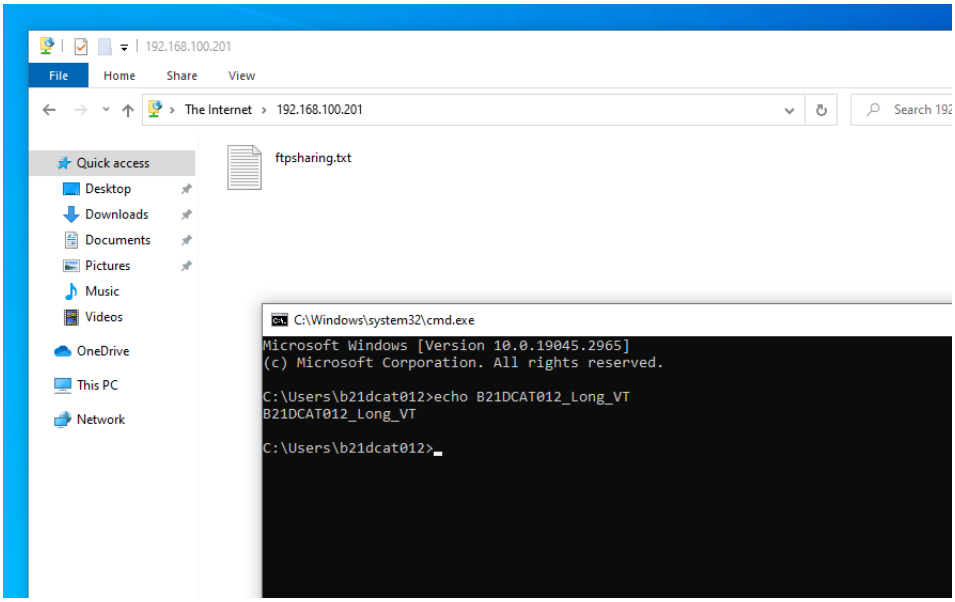


- File này sau đó có thể được mở bằng Wireshark như hình dưới.

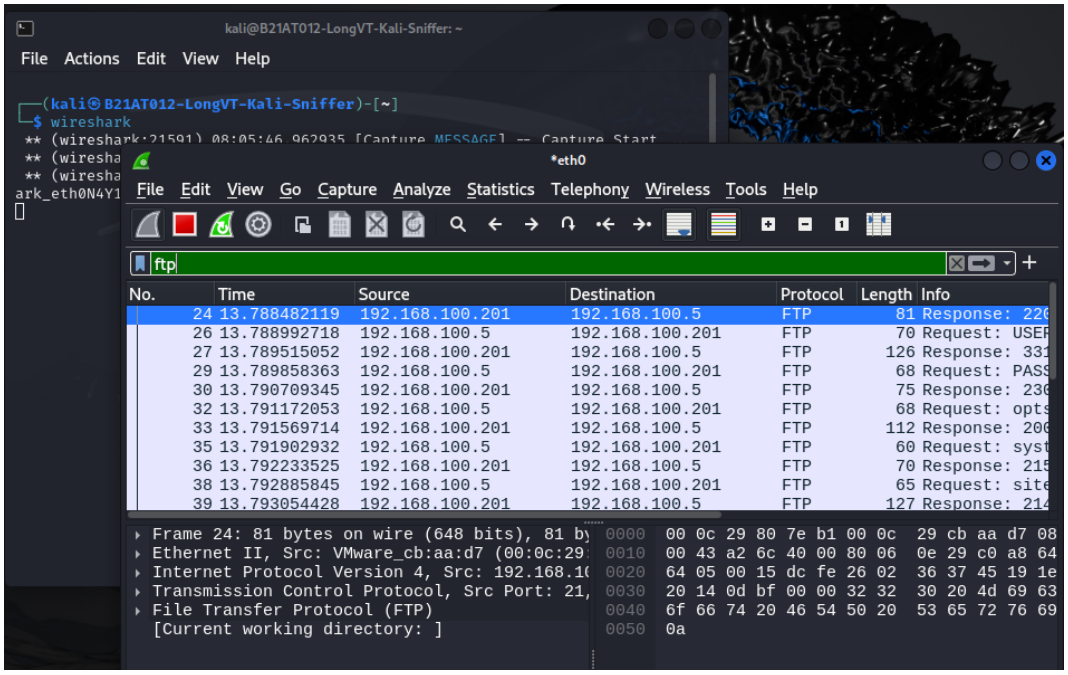


– Sử dụng Wireshark để bắt và phân tích các gói tin:

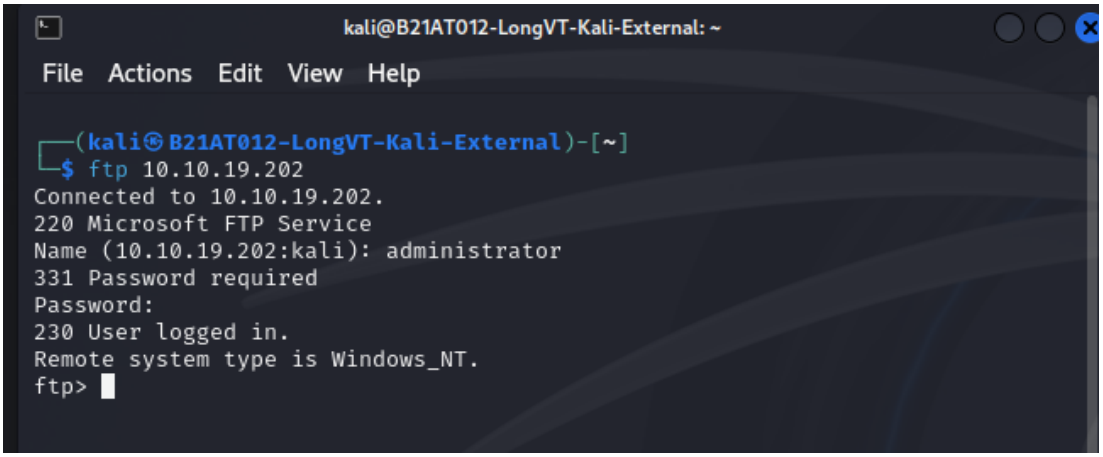
- Khởi động Wireshark trên Sniffer, chọn interface là eth0 rồi bấm Start capture.
- Khởi động Windows 10 attack rồi dùng gõ ftp://192.168.100.201 để truy cập nội dung thư mục FTP của Windows Server Internal.



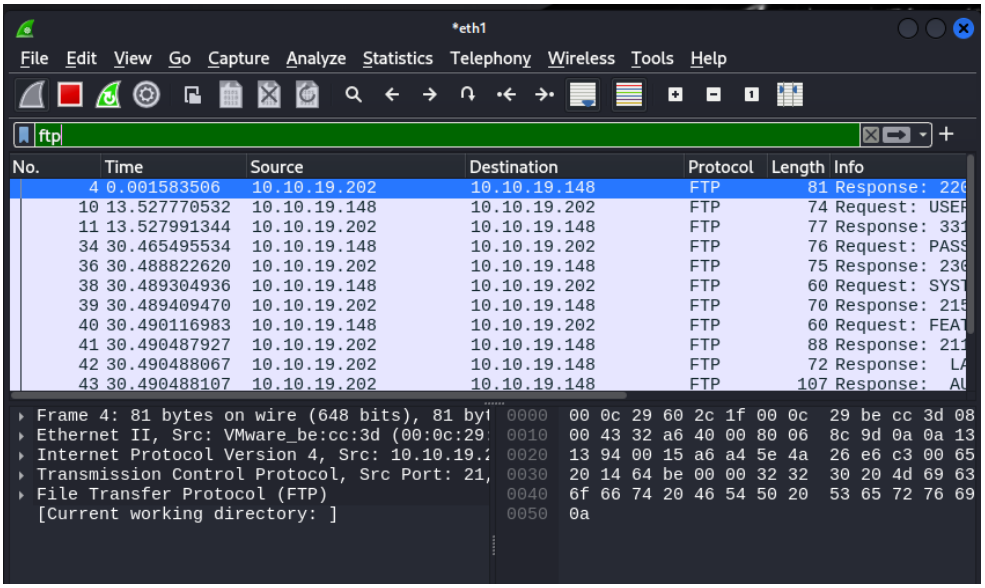
- Kết quả, Wireshark bắt được các gói tin ftp như hình dưới. 192.168.100.5 là địa chỉ IP của Windows 10, còn 192.168.100.201 là địa chỉ IP của Windows Server Internal.
- User anonymous và password là tên đăng nhập mặc định của FTP, do sinh viên đã cấu hình máy chủ FTP chấp nhận người dùng ẩn danh (anonymous).



- Tiếp theo, khởi động lại Wireshark rồi chọn capture giao diện là eth1.

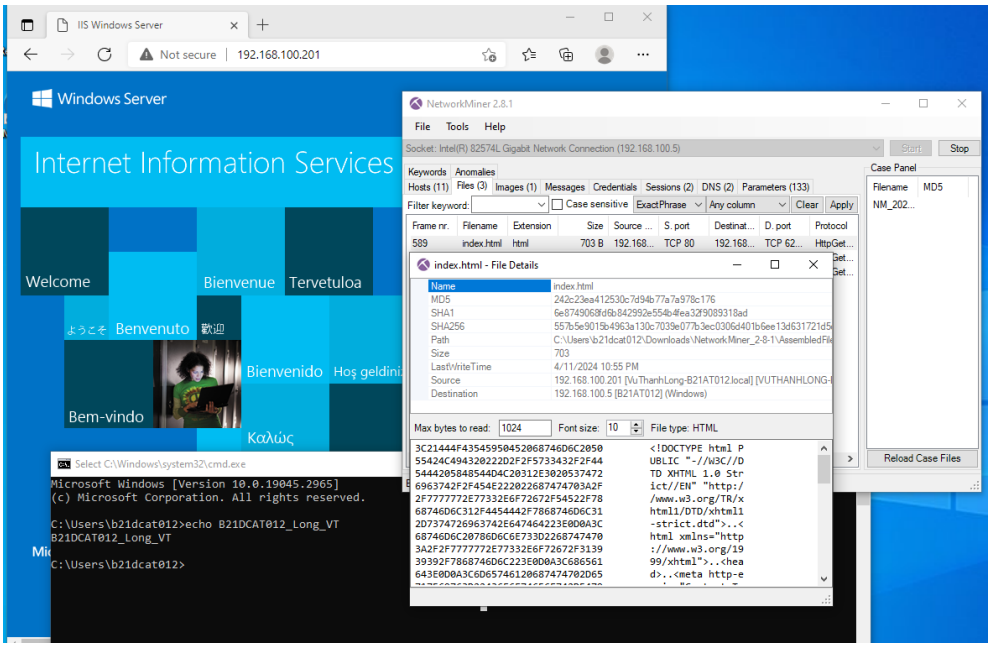


- Kết quả, thu được các gói tin ftp tương tự

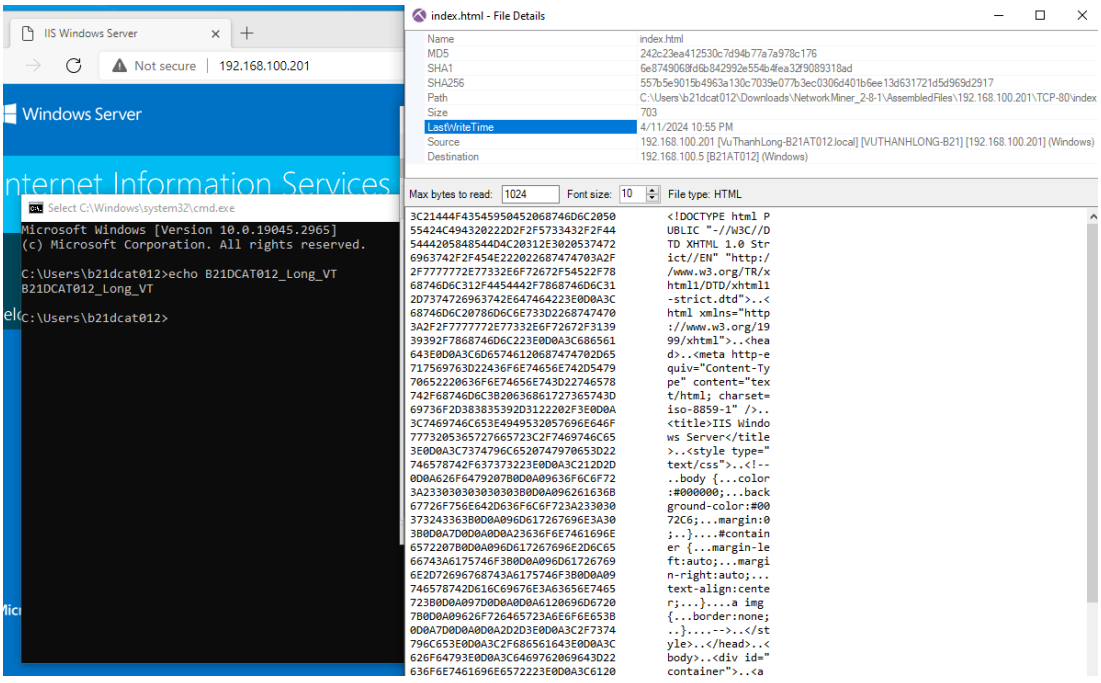


– Sử dụng Network Miner để bắt và phân tích các gói tin:

- Trước hết tải và giải nén Network Miner. Sinh viên chạy NetworkMiner.exe với quyền quản trị viên.
- Lựa chọn interface là Socket: Intel® PRO/1000MT Network Connection(192.168.100.5) rồi bấm Start để bắt đầu bắt các gói tin.
- Truy cập http://192.168.100.201 trên trình duyệt để mở trang web mặc định của máy chủ Windows Server Internal.
- Kết quả, bắt được tệp index.html như hình dưới.



- Thông tin cụ thể của tệp index.html ở hình dưới.



III. Tài liệu tham khảo:

tcpdump manpage: https://www.tcpdump.org/manpages/

Wireshark documentation: https://www.wireshark.org/docs/wsug_html_chunked/