**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

****

**BÁO CÁO BÀI THỰC HÀNH**

**HỌC PHẦN: THỰC TẬP CƠ SỞ**

**MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 3.1**

**BẮT VÀ PHÂN TÍCH GÓI TIN TRONG MẠNG**

Sinh viên thực hiện:Ngô Quang Thắng – B22DCAT287

Giảng viên hướng dẫn: Quản Trọng Thế

**HỌC KỲ 2 NĂM HỌC 2024-2025**

**MỤC LỤC**

[CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH 4](#_Toc196077048)

[1.1 Mục đích 4](#_Toc196077049)

[1.2 Tìm hiểu lý thuyết 4](#_Toc196077050)

[1.2.1. Sniffer là gì? 4](#_Toc196077051)

[1.2.2. Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Tcpdump 4](#_Toc196077052)

[1.2.3. Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Wireshark 5](#_Toc196077053)

[1.2.4. Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Network Miner 6](#_Toc196077054)

[1.2.5. Một số điều cần biết thêm 7](#_Toc196077055)

[CHƯƠNG 2. NỘI DUNG THỰC HÀNH 9](#_Toc196077056)

[2.1 Chuẩn bị môi trường 9](#_Toc196077057)

[2.2 Các bước thực hiện 10](#_Toc196077058)

[2.2.1 Sử dụng tcpdump 10](#_Toc196077059)

[2.2.2 Sử dụng Wireshark để bắt và phân tích các gói tin 15](#_Toc196077060)

[2.2.3 Sử dụng Network Miner để bắt và phân tích các gói tin 19](#_Toc196077061)

[TÀI LIỆU THAM KHẢO 22](#_Toc196077062)

**DANH MỤC HÌNH ẢNH**

[Hình 1: Topo mạng của máy ảo 9](#_Toc196077258)

[Hình 2: Cấu hình ip máy sniffer 10](#_Toc196077259)

[Hình 3: Kiểm tra interfaces của máy Linux Sniffer 11](#_Toc196077260)

[Hình 4: Chế độ hỗn hợp trên máy Linux Sniffer 11](#_Toc196077261)

[Hình 5: Thực hiện nghe tcp trên dải eth1 12](#_Toc196077262)

[Hình 6: Thực hiện ping vảo dải internal từ máy Windows 12](#_Toc196077263)

[Hình 7: Thực hiện ping vào dải mạng internal từ máy Ubuntu 12](#_Toc196077264)

[Hình 8: Lắng nghe tcp dải mạng internal từ máy Linux Sniffer 13](#_Toc196077265)

[Hình 9: Thực hiện ping vào dải mạng external từ máy Ubuntu 13](#_Toc196077266)

[Hình 10: Thực hiện ping vào dải mạng external từ máy Windows 13](#_Toc196077267)

[Hình 11: Lắng nghe tcp dải mạng external từ máy Linux Sniffer 14](#_Toc196077268)

[Hình 12: Đọc gói tin bắt được trên dải mạng external 14](#_Toc196077269)

[Hình 12: Đọc gói tin bắt được trên dải mạng internal 15](#_Toc196077270)

[Hình 14: Khởi động wireshark 16](#_Toc196077271)

[Hình 15: Bắt gói tin trên dải mạng eth1 16](#_Toc196077272)

[Hình 20: Đọc gói tin trên dải mạng external 19](#_Toc196077273)

[Hình 21: Tải xuống NetworkMiner 19](#_Toc196077274)

[Hình 22: Lựa chọn kết nối địa chỉ ip 20](#_Toc196077275)

[Hình 23: Kết nối tới trang web của Windows Server 20](#_Toc196077276)

[Hình 24: Đọc file index.html đã tìm kiếm 21](#_Toc196077277)

1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH
   1. Mục đích

Bài thực hành này giúp sinh viên nắm được công cụ và cách thức bắt dữ liệu mạng, bao gồm:

1. Sử dụng tcpdump để bắt gói tin mạng

2. Sử dụng được Wireshark để bắt và phân tích gói tin mạng (HTTP/HTTPS/FTP / TCP/IP)

3. Sử dụng Network Miner để bắt và phân tích gói tin mạng

* 1. Tìm hiểu lý thuyết

**1.2.1. Sniffer là gì?**

Sniffer hay packet sniffer là một chương trình phần mềm nghe trộm gói tin (còn gọi là chương trình phân tích mạng, phân tích giao thức hay nghe trộm Ethernet), có khả năng chặn bắt và ghi lại lưu lượng dữ liệu qua một mạng viễn thông số hoặc một phần của một mạng. Khi các dòng dữ liệu di chuyển qua lại trong một mạng, chương trình sẽ chặn bắt các gói tin rồi giải mã và phân tích nội dung của nó theo đặc tả RFC hoặc các đặc tả thích hợp khác.

Tùy theo cấu trúc mạng (hub hay chuyển mạch) mà có thể nghe trộm tất cả hoặc chỉ một phần lưu lượng dữ liệu qua lại từ một máy trong mạng. Đối với mục đích giám sát mạng (network monitoring), có thể theo dõi tất cả các gói tin trong một mạng LAN bằng cách sử dụng một thiết bị chuyển mạch với một cổng theo dõi (lặp lại tất cả các gói tin đi qua các cổng của thiết bị chuyển mạch).

**1.2.2. Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Tcpdump**

Tcpdump là một công cụ dòng lệnh được sử dụng để ghi lại và phân tích gói tin trên mạng. Nó cho phép bạn theo dõi lưu lượng mạng đi qua một giao diện cụ thể trên hệ thống của bạn. Bằng cách sử dụng các cú pháp và tùy chọn khác nhau, bạn có thể lọc và hiển thị các gói tin theo nhiều tiêu chí khác nhau như địa chỉ IP, cổng, giao thức, và nhiều hơn nữa. Tcpdump là một công cụ mạnh mẽ được sử dụng rộng rãi trong quản trị hệ thống và mạng để chẩn đoán và gỡ lỗi vấn đề liên quan đến mạng.

Tcpdump sẽ giúp bạn phân các gói dữ liệu phù hợp với dòng lệnh mang theo, cụ thể:

- Bắt bản tin và lưu bằng định dạng PCAP (có thể đọc bởi wireshark)

- Nhìn thấy trực tiếp các bản tin điều khiển hệ thống Linux sử dụng

wireshark, xem chi tiết remote packet capture using Wireshark và tcmpdump

- Có thể nhìn thấy các bản tin trên DUMP trên terminal

- Tạo các bộ lọc Filter để bắt bản tin cần thiết như: http, ssh, fpt…

- Ngoài ra tcmpdump còn sử dụng nhiều option khác nhau nữa

Định dạng chung của một dòng giao thức tcpdump:

*time-stamp src > dst: flags data-seqno ack window urgent options*

Trong đó:

- Time-stamp: hiển thị thời gian gói tin được capture.

- Src và dst: hiển thị địa IP của người gửi và người nhận.

- Cờ Flag thì bao gồm các giá trị sau:

+ S(SYN): Được sử dụng trong quá trình bắt tay của giao thức TCP.

+ .(ACK): Được sử dụng để thông báo cho bên gửi biết là gói tin đã nhận được dữ liệu thành công.

+ F(FIN): Được sử dụng để đóng kết nối TCP.

+ P(PUSH): Thường được đặt ở cuối để đánh dấu việc truyền dữ liệu.

+ R(RST): Được sử dụng khi muốn thiết lập lại đường truyền.

- Data-sqeno: Số sequence number của gói dữ liệu hiện tại.

- ACK: Mô tả số sequence number tiếp theo của gói tin do bên gởi truyền (số sequence number mong muốn nhận được).

- Window: Vùng nhớ đệm có sẵn theo hướng khác trên kết nối này.

- Urgent: Cho biết có dữ liệu khẩn cấp trong gói tin.

Cách hoạt động của Tcpdump

TCPdump là một công cụ dòng lệnh được sử dụng để theo dõi và phân tích gói tin trên mạng. Nó hoạt động bằng cách lắng nghe và ghi lại các gói tin mạng đang đi qua một giao diện mạng cụ thể trên một máy tính. Khi được chạy, TCPdump sẽ hiển thị thông tin về các gói tin này, bao gồm địa chỉ nguồn và đích, loại giao thức, dữ liệu payload, và nhiều thông tin khác. Người dùng có thể sử dụng các tùy chọn và bộ lọc để tinh chỉnh việc theo dõi và phân tích theo nhu cầu cụ thể của họ.

**1.2.3. Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Wireshark**

Wireshark là một công cụ phân tích gói tin mạng mạnh mẽ và đa năng. Nó cho phép bạn chụp, xem xét và phân tích gói tin trên mạng. Wireshark hỗ trợ nhiều loại giao thức mạng và cung cấp các tính năng như lọc gói tin, phân tích luồng dữ liệu, và đồ thị hoạt động mạng. Công cụ này thường được sử dụng để chẩn đoán và gỡ lỗi vấn đề liên quan đến mạng, cũng như để nghiên cứu bảo mật mạng và kiểm tra hiệu suất mạng. Wireshark có giao diện đồ họa dễ sử dụng và được hỗ trợ trên nhiều hệ điều hành khác nhau.

Wireshark là một phần mềm dùng để phân tích và giám sát lưu lượng mạng. Dưới đây là một số chức năng chính của Wireshark:

- **Phân tích Gói Tin**: Wireshark cho phép bạn theo dõi và phân tích từng gói tin dữ liệu trên mạng. Bạn có thể xem các thông tin chi tiết như nguồn, đích, loại gói tin, dữ liệu payload và nhiều thông tin khác.

- **Đánh giá Hiệu suất Mạng**: Wireshark cung cấp thông tin về thời gian phản hồi (response time), độ trễ (latency), và các thống kê khác, giúp đánh giá hiệu suất của mạng.

- **Phân tích Giao thức**: Wireshark hỗ trợ nhiều giao thức mạng khác nhau. Bạn có thể xem và phân tích giao thức HTTP, TCP, UDP, IP, DNS, và nhiều giao thức khác.

- **Điều tra Vấn đề Mạng**: Khi xảy ra vấn đề mạng, Wireshark là một công cụ mạnh mẽ để phân tích và xác định nguyên nhân của sự cố.

**- Bảo mật Mạng**: Wireshark có thể được sử dụng để phát hiện các hoạt động độc hại trên mạng. Nó cho phép bạn xem gói tin để phát hiện các tấn công mạng, như phishing hoặc kiểm soát truy cập không được ủy quyền.

- **Giáo dục và Học tập**: Wireshark là một công cụ hữu ích cho sinh viên, chuyên gia mạng, và người quan tâm đến việc hiểu rõ cách mạng hoạt động. Nó cung cấp một cách thức thực hành để nắm bắt và hiểu các khái niệm mạng.

Cách hoạt động của Wireshark

Như đã đề cập ở trên, đây là một công cụ dùng để capture và phân tích các packet. Nó capture các lưu lượng mạng trên mạng cục bộ, sau đó sẽ lưu trữ nó để phân tích offline.

Có thể capture các lưu lượng mạng từ các kết nối Ethernet, Bluetooth, Wireless (IEEE.802.11), Token Ring, Frame Relay…

Wireshark cho phép thiết lập filter (bộ lọc) trước khi bắt đầu capture hoặc thậm chí là trong quá trình phân tích. Do đó, ta có thể thu hẹp phạm vi tìm kiếm trong quá trình theo dõi mạng.

**1.2.4. Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Network Miner**

NetworkMiner là một công cụ phân tích mạng dành cho Windows. Nó cho phép người dùng thu thập dữ liệu từ mạng và phân tích thông tin như các máy chủ, giao thức, trình duyệt web, và nhiều hơn nữa. NetworkMiner tự động phát hiện các hoạt động mạng như kết nối TCP, truy vấn DNS và nó cũng có thể hỗ trợ trong việc phát hiện và phân loại các tập tin được truyền qua mạng. Nó thường được sử dụng để phát hiện các mối đe dọa mạng và phân tích dữ liệu từ gói tin đã chụp.

Những điểm nổi bật của NetworkMiner phải kể đến:

- Giám sát hầu như mọi gói tin trao đổi ra vào máy chủ, trong đó cho phép phát hiện ảnh, các file dữ liệu và tài khoản đăng nhập.

- Dữ liệu hiển thị ở dạng rất dễ hiểu.

- Dung lượng nhẹ (phiên bản 2.6 sau khi giải nén chỉ chiếm 47,9 MB), không cần cài đặt (chỉ cần tải về, giải nén là sử dụng được ngay) và rất dễ sử dụng.

- Có hai phiên bản miễn phí và pro (trả phí) để lựa chọn. Trong đó, phiên bản trả phí cho phép tìm kiếm trực tuyến thông tin về địa chỉ IP.

- Khả năng phân tích email trao đổi qua các giao thức SMTP, POP3 và IMAP.

- Nâng cấp khả năng phát hiện mật khẩu, phát hiện trao đổi dữ liệu qua giao thức FTP, những dấu hiệu bất thường trong trao đổi dữ liệu qua giao thức HTTP và HTTP/2.

- Nâng cấp khả năng tương thích với hệ điều hành Linux.

- Hỗ trợ phân tích các gói tin qua giao thức GRE, PPPoE, VXLAN, OpenFlow, MPLS và EoMPLS.

Cách hoạt động của NetworkMiner

NetworkMiner là một công cụ phân tích mạng có khả năng thu thập dữ liệu từ gói tin mạng trên một giao diện cụ thể trên máy tính.

Sau đó, nó phân tích các gói tin để trích xuất thông tin quan trọng như địa chỉ IP, tên miền, thông tin trình duyệt web và các tập tin được truyền qua mạng.

Dữ liệu được hiển thị trên giao diện người dùng và có thể được lưu trữ dưới dạng tập tin PCAP để phân tích và thẩm định sau này.

**1.2.5. Một số điều cần biết thêm**

Chế độ hỗn độn trên card mạng:

"Chế độ hỗn độn" (hay còn gọi là "promiscuous mode") trên một card mạng là một trạng thái hoạt động đặc biệt của card mạng. Khi một card mạng hoạt động trong chế độ hỗn độn, nó sẽ bắt đầu nhận tất cả các gói tin trên mạng, bao gồm cả những gói tin không địa chỉ cho chính nó.

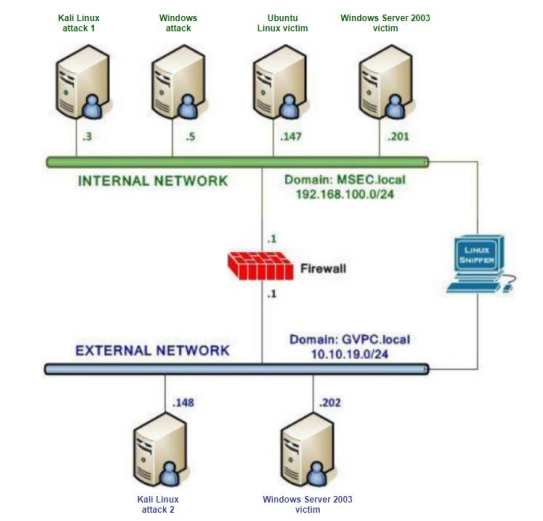
Chế độ hỗn độn thường được sử dụng cho các mục đích giám sát, phân tích mạng, hoặc để phát hiện các vấn đề về bảo mật mạng.

Kích hoạt chế độ hỗn độn trên Linux:

*sudo ifconfig promisc*

1. NỘI DUNG THỰC HÀNH
   1. Chuẩn bị môi trường

* Phần mềm VMWare Workstation( hoặc các phần mềm hỗ trợ ảo hóa khác).
* Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài thực hành 5 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. **Chú ý:** chỉ cần bật các máy cần sử dụng trong bài lab.
* Topo mạng như đã cấu hình:



Hình 1: Topo mạng của máy ảo

* 1. Các bước thực hiện

**2.2.1 Sử dụng tcpdump**

a) Các bước thực hiện

o Trên máy Windows attack trong mạng Internal, đăng nhập Linux Sniffer và xem tất cả các interfaces trong hệ thống (root@bt:~#ifconfig -a)

* Cấu hình mạng của máy Linux Sniffer:

*# Interface eth0*

*auto eth0*

*iface eth0 inet static*

*address 10.10.19.148*

*netmask 255.255.255.0*

*gateway 10.10.19.1*

*dns-nameservers 8.8.8.8 8.8.4.4*

*# Interface eth1*

*auto eth1*

*iface eth1 inet static*

*address 192.168.100.10*

*netmask 255.255.255.0*

*gateway 192.168.100.1*

*dns-nameservers 8.8.8.8 8.8.4.4*



Hình 2: Cấu hình ip máy sniffer

* Xem tất cả các interfaces trong hệ thống :

*ip -a*

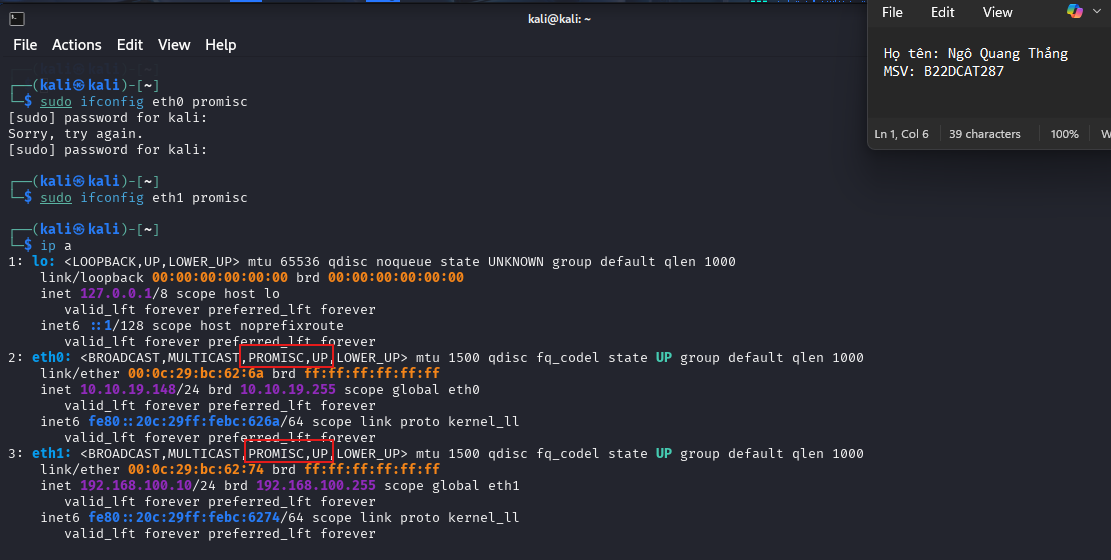


Hình 3: Kiểm tra interfaces của máy Linux Sniffer

o Trên máy Windows attack trong mạng Internal, kích hoạt các interfaces(eth0, eth1) hoạt động ở chế độ hỗn hợp:

*sudo ifconfig eth0 promisc*

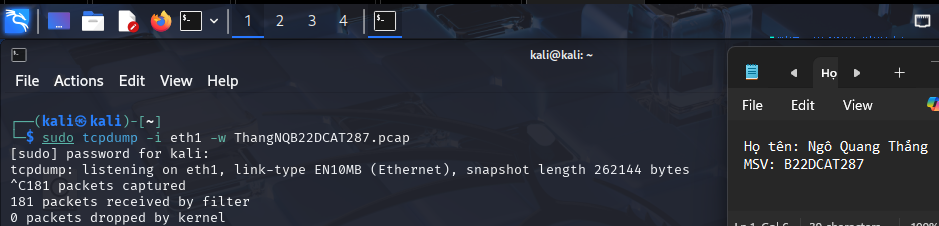
*sudo ifconfig eth1 promisc*



Hình 4: Chế độ hỗn hợp trên máy Linux Sniffer

* Khởi động tcpdump, bắt gói tin trên dải mạng 192.168.100.0/24 và gửi vào một file(thời gian chờ dữ liệu trong khoảng 5 phút).

*sudo tcpdump -i eth1 -w ThangNQB22DCAT287.pcap*

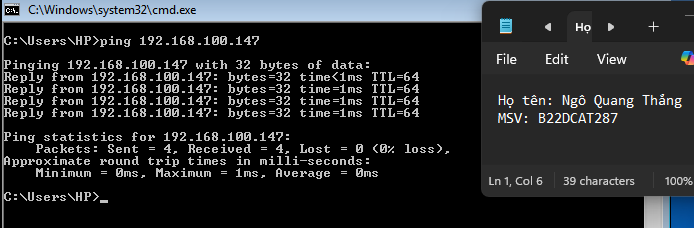


Hình 5: Thực hiện nghe tcp trên dải eth1

o Trên máy Window victim, đăng nhập Window Server 2003 và tiến hành ping đến dải mạng internal và dải mạng external

* Dải mạng internal:
  + Từ máy Windows ping đền dải mạng internal

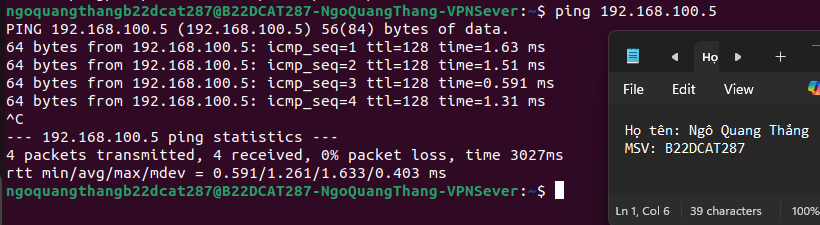
*ping 192.168.100.147*



Hình 6: Thực hiện ping vảo dải internal từ máy Windows

* + Máy ubuntu internal ping đến dải mạng:

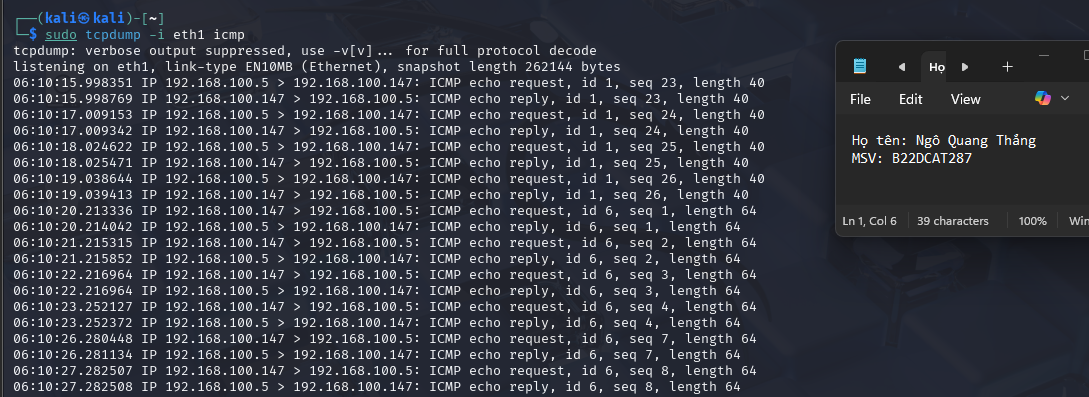
*ping 192.168.100.5*



Hình 7: Thực hiện ping vào dải mạng internal từ máy Ubuntu

* + Từ máy Linux Sniffer theo dõi các gói tin trên dải mạng internal

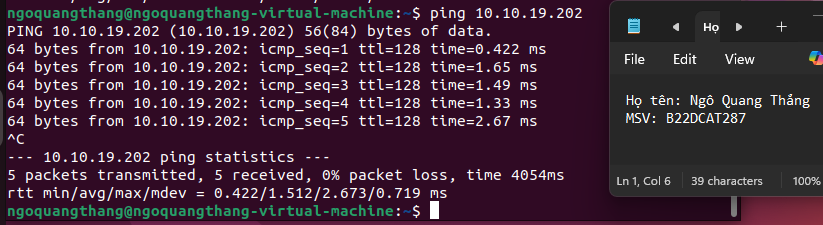
*sudo tcpdump -i eth1 icmp*



Hình 8: Lắng nghe tcp dải mạng internal từ máy Linux Sniffer

* Dải mạng external
  + Trên máy Ubuntu External ping đến dải mạng

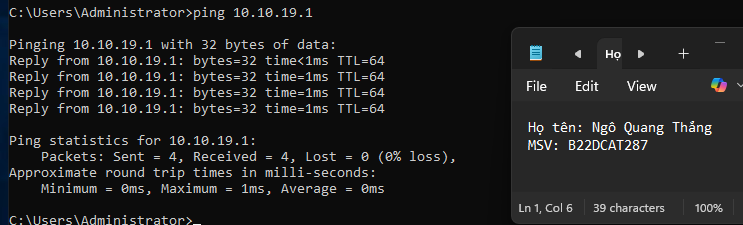
*ping 10.10.19.202*



Hình 9: Thực hiện ping vào dải mạng external từ máy Ubuntu

* + Trên máy Windows Sever ping đến dải mạng

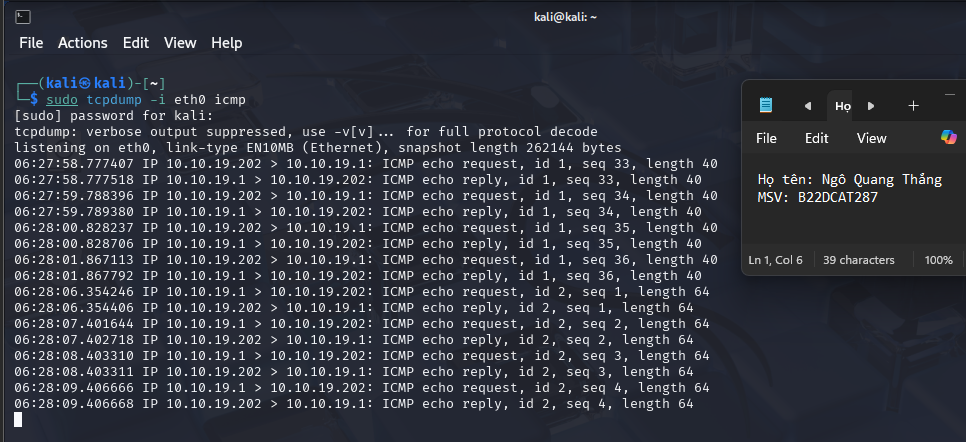
*ping 10.10.19.1*



Hình 10: Thực hiện ping vào dải mạng external từ máy Windows

* + Từ máy Linux Sniffer theo dõi các gói tin trên dải mạng external

*sudo tcpdump -i eth0 icmp*

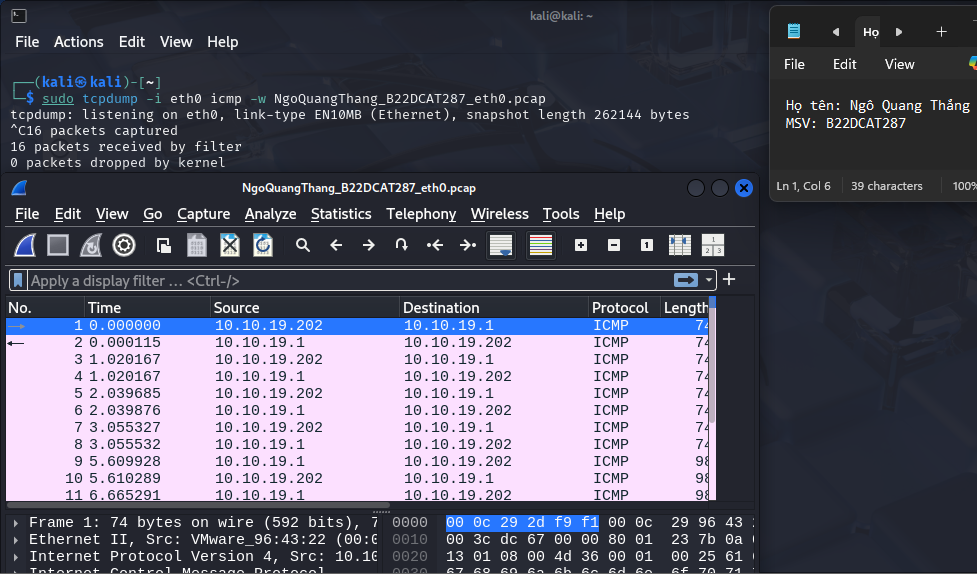


Hình 11: Lắng nghe tcp dải mạng external từ máy Linux Sniffer

o Trên máy Window attack, tiến hành bắt gói tin bằng tcpdump, và lưu dữ liệu vào file pcap.

* Với dải mạng external bắt các gói tin icmp:

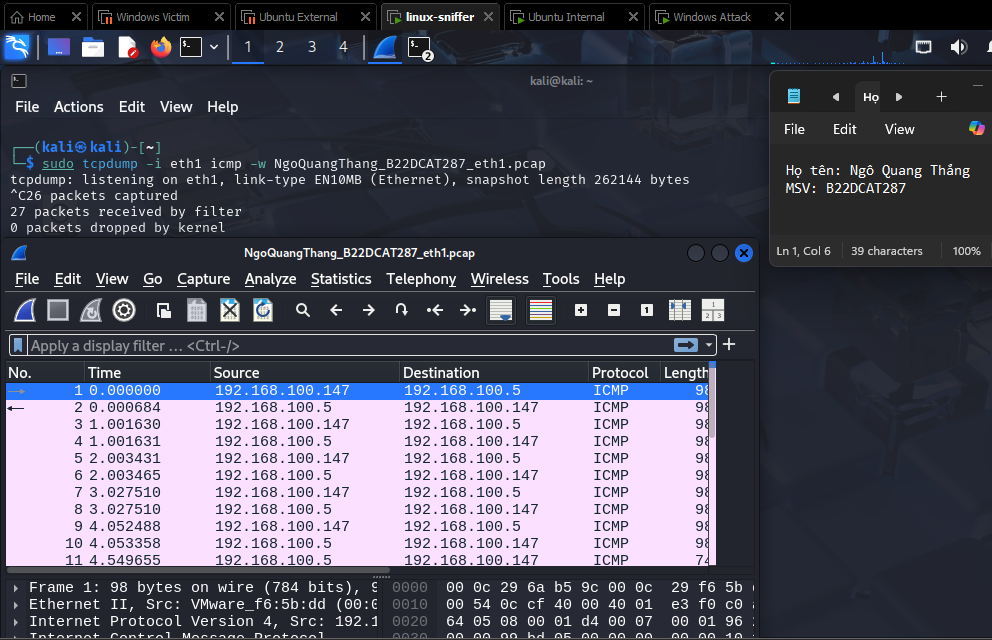
*sudo tcpdump -i eth0 icmp -w NgoQuangThang\_B22DCAT287\_eth0.pcap*



Hình 12: Đọc gói tin bắt được trên dải mạng external

* Với dải mạng internal bắt các gói tin icmp:

*sudo tcpdump -i eth1 icmp -w NgoQuangThang\_B22DCAT287\_eth1.pcap*



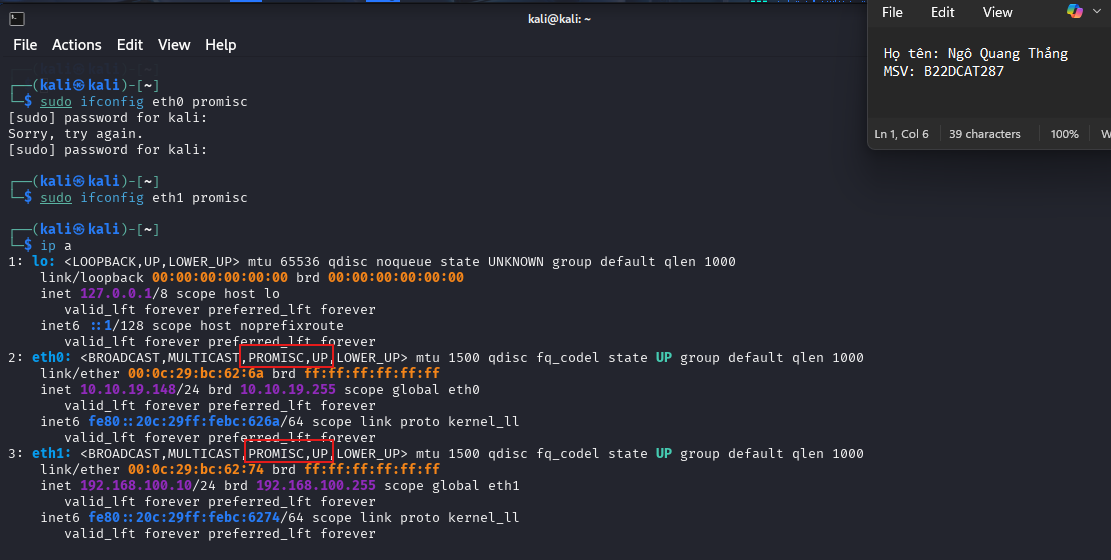
Hình 12: Đọc gói tin bắt được trên dải mạng internal

**2.2.2 Sử dụng Wireshark để bắt và phân tích các gói tin**

a) Các bước thực hiện

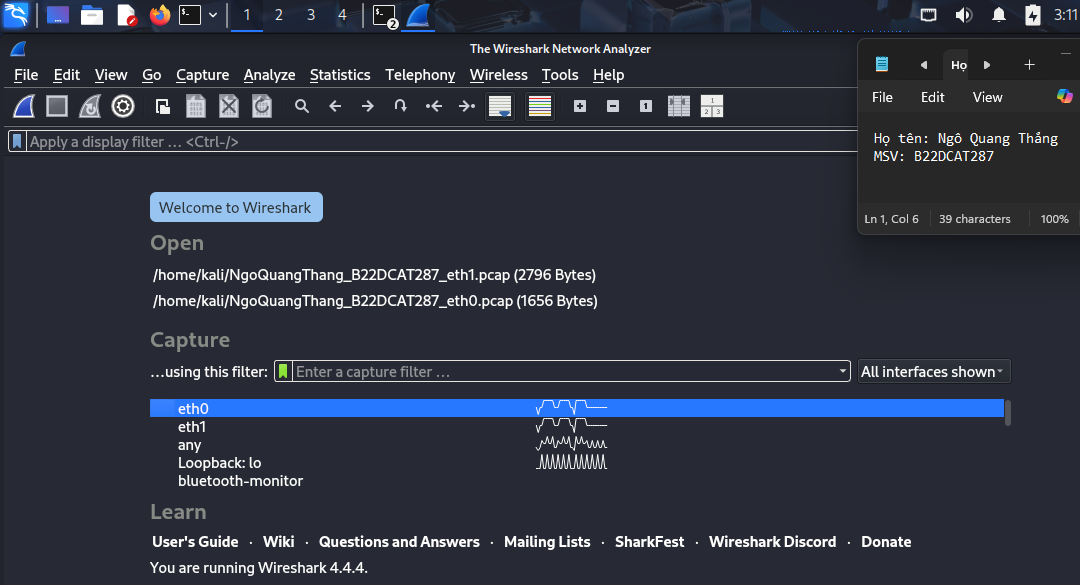
o Có thể tải Wireshark ở đây: <http://www.wireshark.org/download.html>

o Trên máy Windows attack, bật các interfaces eth0, eth1



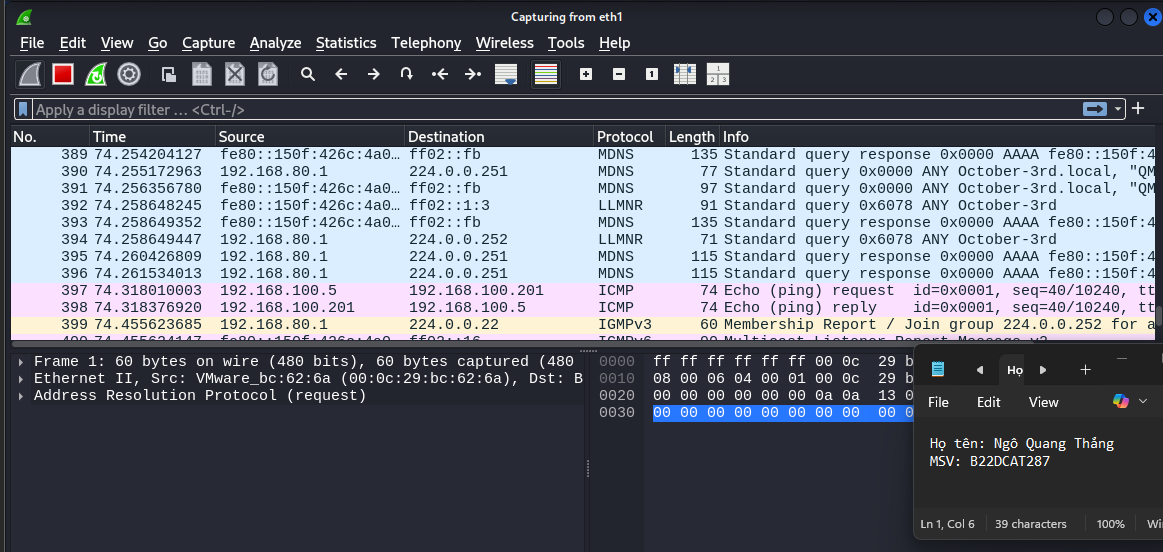
Hình 13: Cấu hình interfaces hỗn hợp eth1,eth0

* Khởi động wireshark



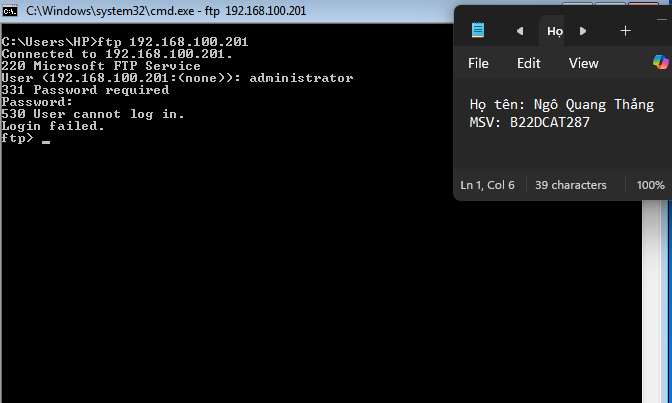
Hình 14: Khởi động wireshark

* Trong Capture Interfaces chọn Start ở dòng eth1 để bắt gói tin trên dải mạng 192.168.100.0



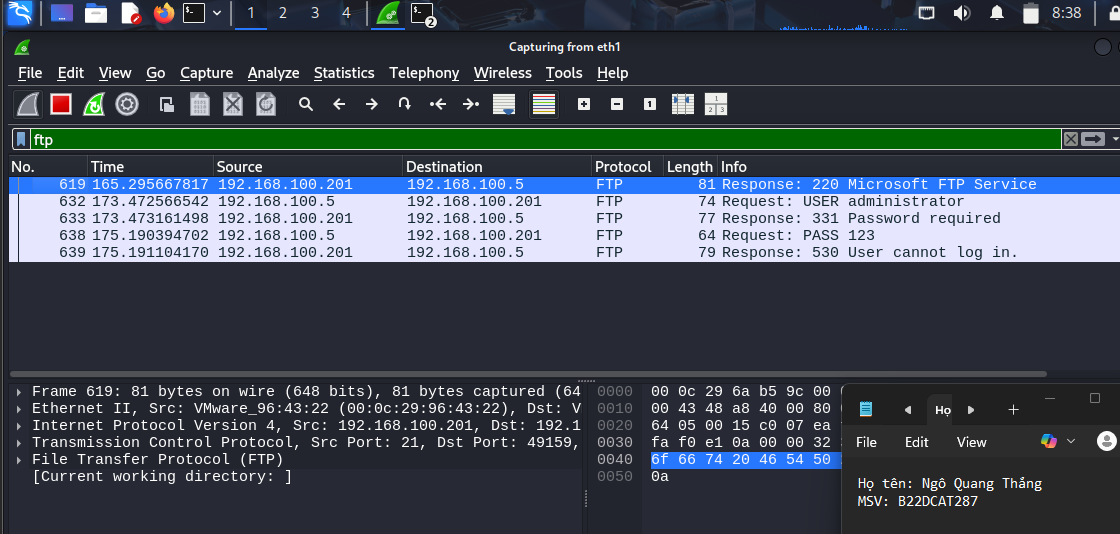
Hình 15: Bắt gói tin trên dải mạng eth1

o Trên máy Windows 7 victim kết nối tới ftp server (C:\ftp 192.168.100.201)



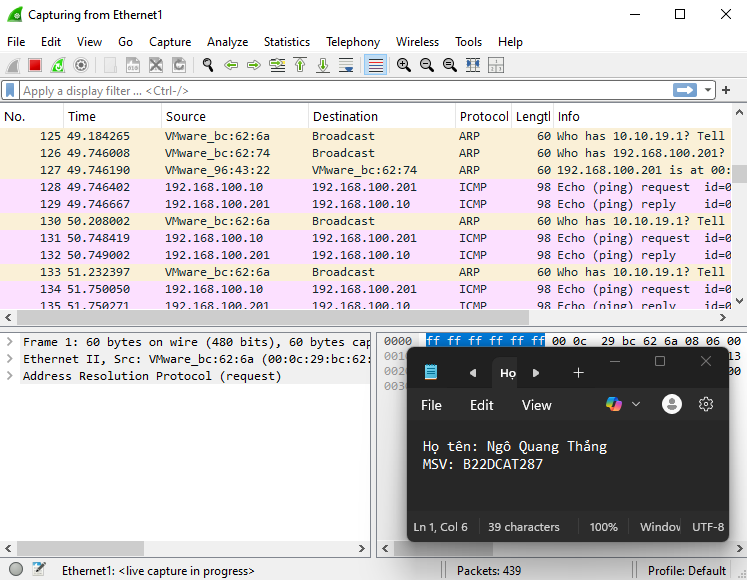
Hình 16: Kết nối ftp đến WindowsSever

o Trên Linux Sniffer dừng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp (Tại ô lọc theo yêu cầu ghi “ftp”)



Hình 17: Lọc gói tin theo giao thức ftp

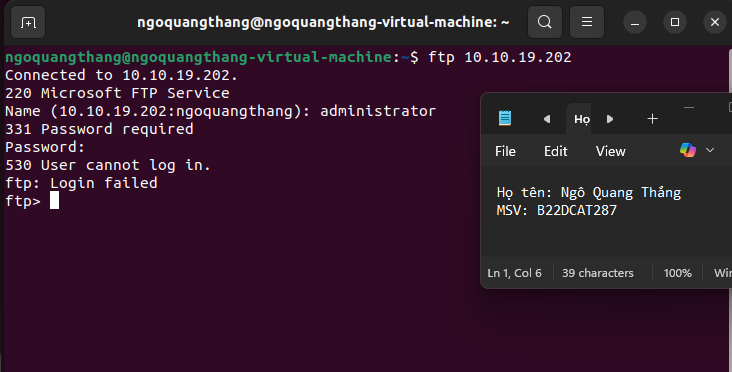
o Trên máy Windows attack, trong Capture Interfaces chọn Start ở dòng eth1 để bắt gói tin trên dải mạng 192.168.100.0



Hình 18: Đọc gói tin dải mạng 192.168.100.0 trên máy Windows

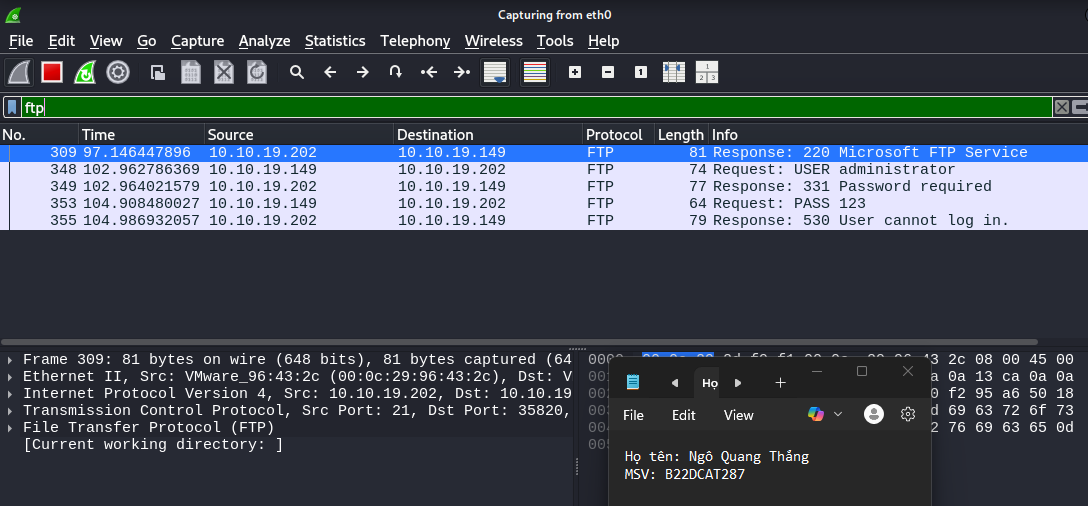
o Trên máy Window Server 2003 victim, kết nối với ftp server

*ftp 10.10.19.202*



Hình 19: Kết nối ftp trên dải mạng external

o Trên Linux Sniffer dừng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp(Tại ô lọc theo yêu cầu ghi “ftp”)



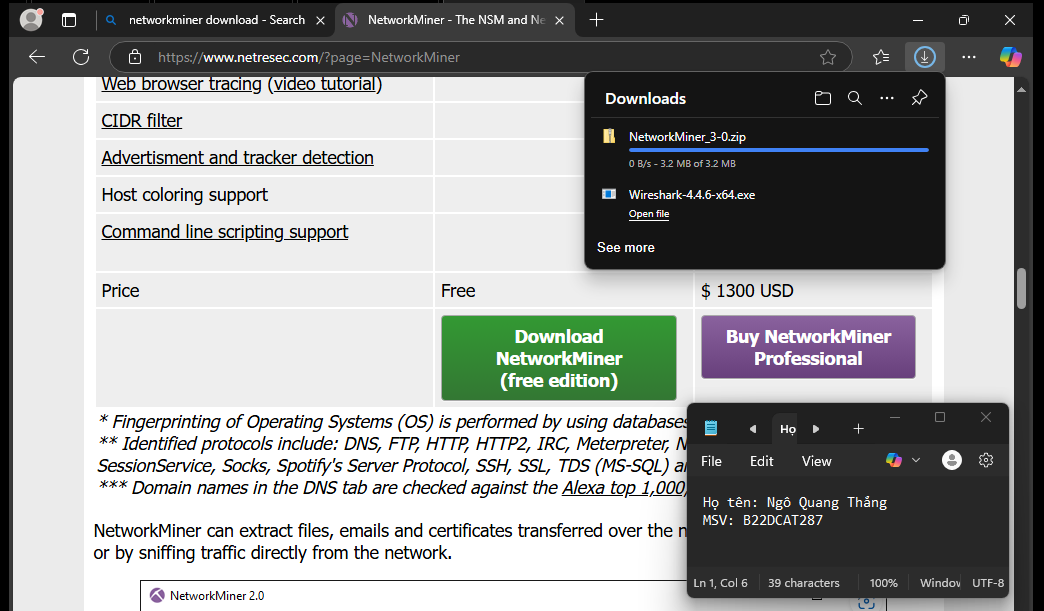
Hình 20: Đọc gói tin trên dải mạng external

**2.2.3 Sử dụng Network Miner để bắt và phân tích các gói tin**

a) Các bước thực hiện

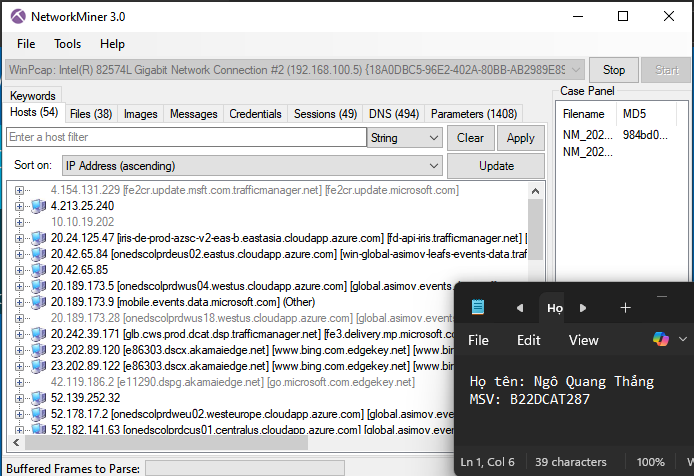
o Thực hiện tải xuống Network Miner

*https://www.netresec.com/?page=NetworkMiner*



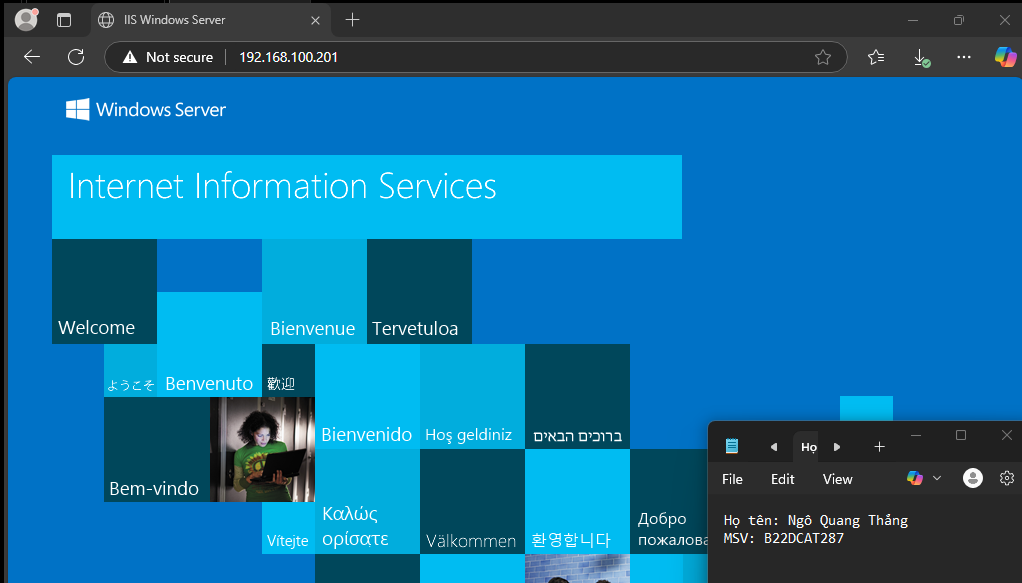
Hình 21: Tải xuống NetworkMiner

o Trên máy Windows 7 Internal Attack khởi động Network Miner và chọn Socket: Intel® PRO/1000MT Network Connection(192.168.100.5) và bắt đầu bắt gói tin.



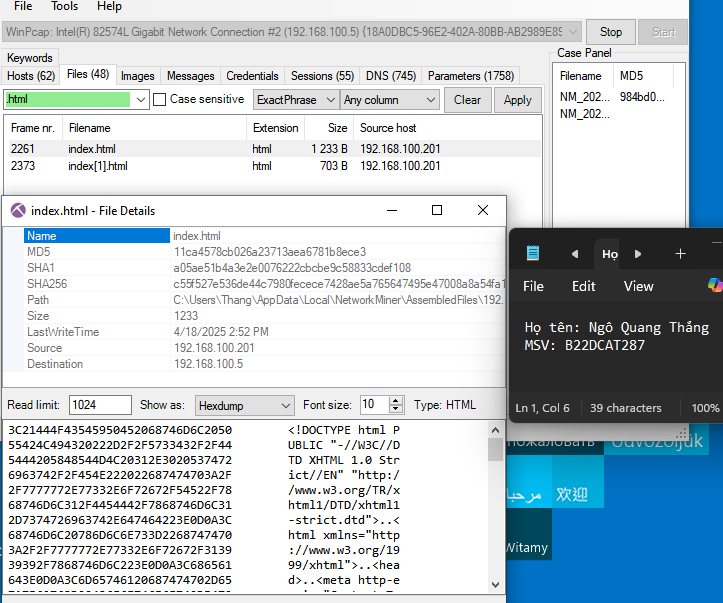
Hình 22: Lựa chọn kết nối địa chỉ ip

* Sử dụng Internet Explorer để kết nối đến trang web của Windows 2003 Server Internal Victim: http://192.168.100.201/. Sau đó dừng quá trình bắt gói tin.



Hình 23: Kết nối tới trang web của Windows Server

o Trong Network Miner, chọn File/ index.html để xem dữ liệu gói tin vừa bắt được.



Hình 24: Đọc file index.html đã tìm kiếm

TÀI LIỆU THAM KHẢO

1. Chương 4, Bài giảng Kỹ thuật theo dõi giám sát an toàn mạng, HVCN BCVT 2021
2. <https://www.tcpdump.org/index.html#documentation>
3. <https://www.wireshark.org/docs/wsug_html/>
4. https://docs.securityonion.net/en/2.3/networkminer.html#