HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÁO CÁO BÀI THỰC HÀNH
THỰC TẬP CƠ SỞ
Bài 08: Bắt dữ liệu mạng

Họ và tên: Nguyễn Huy Quang

Mã sinh viên: B20DCAT144

Giảng viên: Nguyễn Hoa Cương

Hà Nội – 2023

MỤC LỤC

I. Tìm hiểu lý thuyết

1. TCPDUMP

- Là công cụ được phát triển nhằm mục đích nhận diện và phân tích các gói dữ liệu mạng theo dòng lệnh.
- Cho phép khách hàng chặn và hiển thị các gói tin được truyền đi hoặc được nhận diện trên một mạng có sự tham gia của máy tính.
- Là phần mềm bắt gói tin trong mạng làm việc trên hầu hết các phiên bản hệ điều hành Unix/Linux. tcpdump cho phép bắt và lưu lại những gói tin bắt được, từ đó chúng ta có thể sử dụng để phân tích.
- TCPDUMP được xem là trụ cột trong việc gỡ rối và kiểm tra vấn đề kết nối mạng và bảo mật.
- TCPDUMP xuất ra màn hình nội dung các gói tin (chạy trên card mạng mà máy chủ đang lắng nghe) phù hợp với biểu thức logic chọn lọc mà khách hàng nhập vào.
- Với từng loại tùy chọn khác nhau khách hàng có thể xuất những mô tả về gói tin này ra một file "pcap" để phân tích sau, và có thể đọc nội dung của file "pcap" đó với option –r của lệnh TCPDUMP, hoặc sử dụng các phần mềm khác như là : Wireshark.
- Trong trường hợp không có tùy chọn, lệnh TCPDUMP sẽ tiếp tục chạy cho đến khi nào nó nhận được một tín hiệu ngắt từ phía khách hàng. Sau khi kết thúc việc bắt các gói tin, TCPDUMP sẽ báo cáo các cột sau:
  + Packet capture: số lượng gói tin bắt được và xử lý.
  + Packet received by filter: số lượng gói tin được nhận bởi bộ lọc.
  + Packet dropped by kernel: số lượng packet đã bị dropped bởi cơ chế bắt gói tin của hệ điều hành.
- Ưu điểm khi sử dụng tcpdump:
  + Nhìn thấy được các bản tin DUMP trên terminal.
  + Bắt các bản tin và lưu vào định dạng PCAP (có thể đọc được bởi Wireshark).
  + Tạo được các bộ lọc Filter để bắt các bản tin cần thiết, ví dụ: http, ftp, ssh, …
  + Có thể nhìn được trực tiếp các bản tin điều khiển hệ thống Linux sử dụng Wireshark.
  + TCPDUMP là một công cụ vô cùng hữu ích đối với khả năng capturing packets khá mạnh mẽ. Nó hoạt động trên network layer và có thể capture tất cả các packets ra vào máy tính. Ngoài ra, có thể sử dụng TCPDUMP để capture và save các packets tới một file nào đó và phân tích sau.

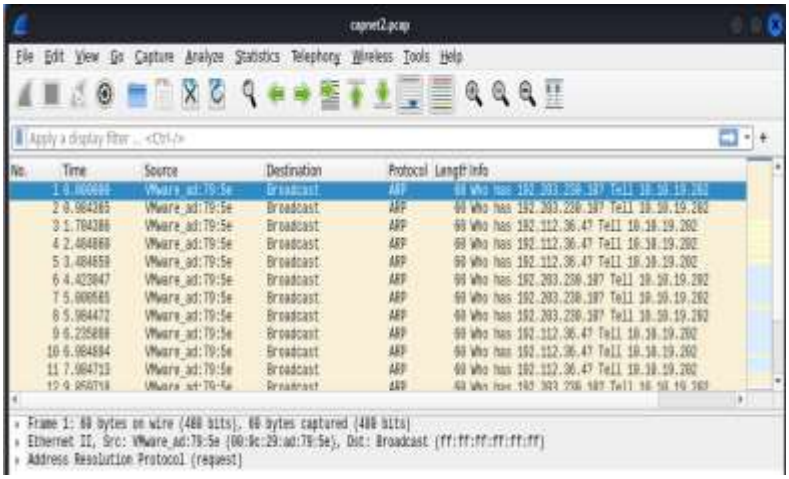
- Một số tùy chọn thông dụng trên TCPDUMP
  + -i: Sử dụng tùy chọn này khi khách hàng muốn bắt các gói tin trên một interface được chỉ định.
  + -D: Khi sử dụng tùy chọn này, TCPDUMP sẽ liệt kê ra tất cả các interface đang hiện hữu trên máy tính mà nó có thể capture được.
  + -n: Khi sử dụng tùy chọn này, TCPDUMP sẽ không phân giải từ địa chỉ IP sang hostname.
  + -v: Tăng số lượng thông tin về gói tin mà bạn có thể nhận được.
  + -s: Định nghĩa snaplength (kích thước) gói tin sẽ lưu lại, sử dụng 0 để mặc định.
  + -x: Hiển thị dữ liệu của gói tin capture dưới dạng mã Hex.

2. Wireshark

- Wireshark là phần mềm phân tích giao thức mạng tin cậy và được sử dụng rộng rãi trên toàn thế giới. Phần mềm giúp bạn nắm được mọi thông số liên quan đến mạng máy tính của người dùng và dữ liệu chi tiết nhất.
- Wireshark là sản phẩm của công ty cùng tên là Wireshark. Đây là một dự án phần mềm mã nguồn mở và được phát hành theo Giấy phép Công cộng GNU (GPL). Người dùng có thể thoải mái sử dụng Wireshark trên bất kỳ số lượng máy tính nào mà không cần lo lắng về khóa cấp phép hoặc chi phí bổ sung.

- Tính năng của wireshark
  + Theo dõi chuyên sâu hàng trăm giao thức. Các giao thức mạng mới sẽ được bổ sung liên tục vào Wireshark mới nhất.
  + Ghi lại hoạt động mạng trong thời gian thực và hỗ trợ phân tích mạng offline.
  + Trình duyệt gói 3 bảng tiêu chuẩn.

+ Wireshark hỗ trợ đa nền tảng: Windows, Linux, MacOS, FreeBSD…
+ Dữ liệu mạng ghi lại sẽ được duyệt thông qua GUI hoặc thông qua chế độ TTY – tiện ích TShark.
+ Sử dụng các bộ lọc hiển thị mạnh nhất hiện nay.
+ Phân tích VoIP toàn diện.
+ Có thể đọc và viết nhiều định dạng file lưu khác nhau như tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer (nén và giải nén).



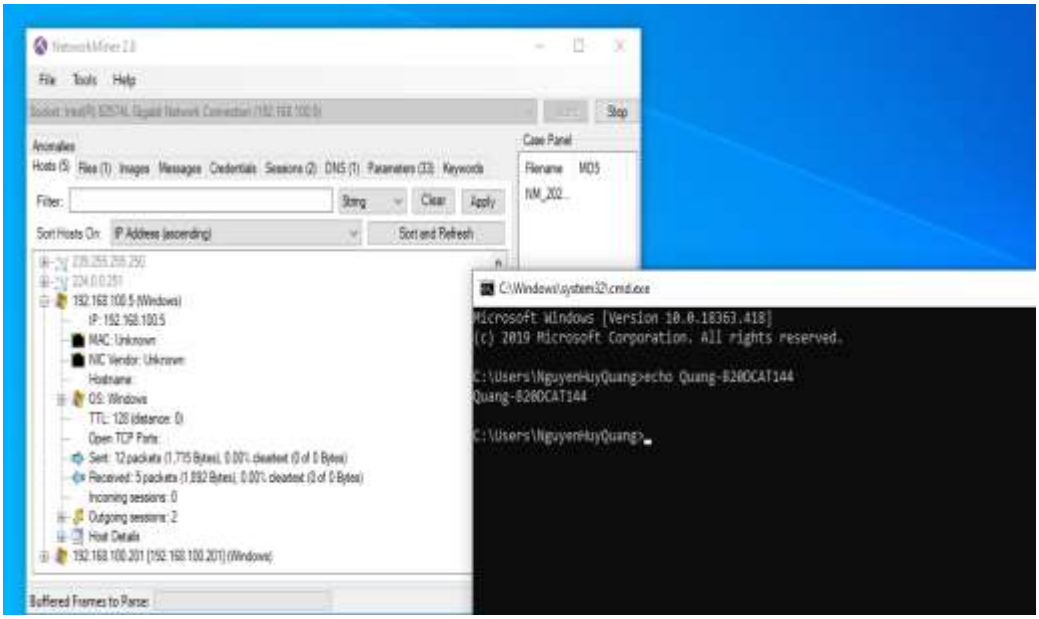
+ File lưu nén bằng gzip sẽ được giải nén trực tiếp.
+ Đọc dữ liệu trực tiếp từ Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI… (phụ thuộc vào hệ điều hành máy tính bạn đang dùng).
+ Hỗ trợ mô tả cho nhiều giao thức, bao gồm IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP và WPA/WPA2.
+ Sử dụng mã màu cho các gói dữ liệu mạng khác nhau để phân tích nhanh, dễ dàng hơn.
+ Xuất dữ liệu phân tích giao thức mạng ra các định dạng phổ biến như XML, PostScript, CSV hoặc văn bản thường.

- Ưu điểm của Wireshark
  + Phân tích chuyên sâu các giao thức mạng.
  + Thu thập dữ liệu từ nhiều gói tin.
  + Hỗ trợ các bộ lọc mạnh mẽ.
  + Cung cấp các phương pháp phân tích trực quan và nhanh chóng.
  + Giải nén nhiều giao thức mạng.
  + Đọc dữ liệu từ nhiều giao thức.

+ Xuất dữ liệu sang nhiều định dạng khác nhau.
+ Wireshark là phần mềm mạng được lựa chọn bởi nhiều đối tượng người dùng, bao gồm các doanh nghiệp kinh doanh hay hoạt động phi lợi nhuận, các tổ chức chính phủ hay trường học, cơ quan khác.

3. Network Miner

- NetworkMiner là một công cụ phân tích mạng (NFAT) mã nguồn mở dành cho Windows (nhưng cũng hoạt động trong Linux / Mac OS X / FreeBSD).
  NetworkMiner có thể được sử dụng như một công cụ thu thập gói / dò tìm 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 cũng có thể phân tích cú pháp tệp PCAP để phân tích ngoại tuyến và tái tạo / tập hợp lại các tệp và chứng chỉ đã truyền từ tệp PCAP.
- NetworkMiner giúp dễ dàng thực hiện Phân tích lưu lượng mạng nâng cao (NTA) bằng cách cung cấp các tạo tác được trích xuất trong giao diện người dùng trực quan. Cách dữ liệu được trình bày không chỉ làm cho việc phân tích đơn giản hơn mà còn tiết kiệm thời gian quý báu cho nhà phân tích.
- Hình ảnh về NetworkMiner



- Tính năng của NetworkMiner
  + Phân tích các tệp tin pcap trong trường hợp ngoại tuyến

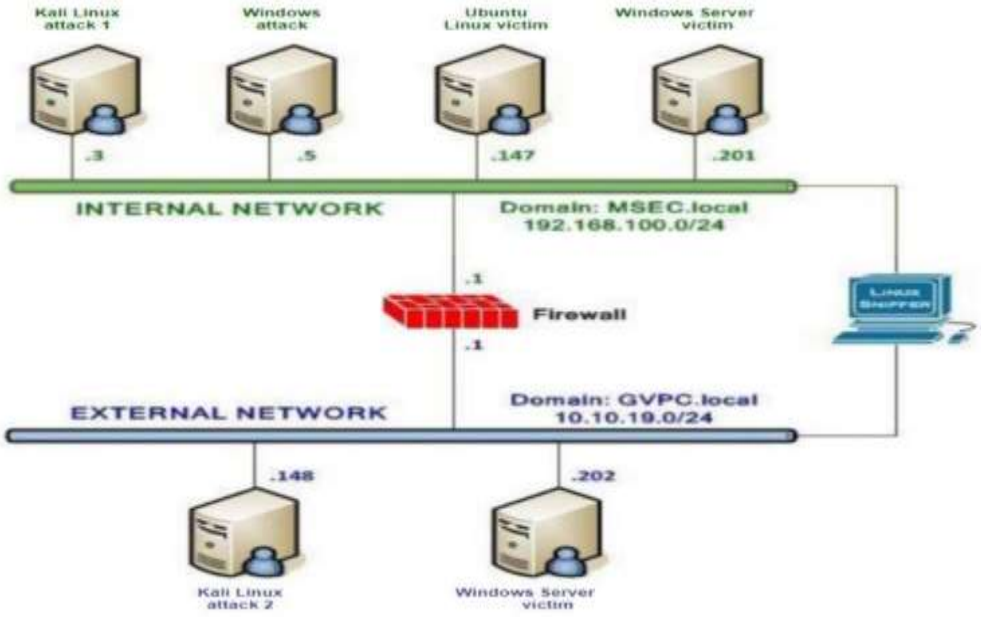
+ Tái tạo các tập tin truyền tải, cấu trúc thư mục hay chứng chỉ từ tệp tin pcap. thu thập dữ liệu (chẳng hạn như chứng cứ) về các host trên mạng, không thu thập dữ liệu về lưu lượng truy cập.
+ Quan tâm đến trung tâm máy chủ (nhóm các thông tin trên từng máy), không tập trung vào gói tin (thông tin về danh sách các gói tin, khung nhìn...).

- NetworkMiner là công cụ tiện dụng trong việc phân tích máy chủ C&C (Command & Control) hay khi kiểm soát lưu lượng truy cập từ mạng lưới botnet.

II. Nội dung thực hành

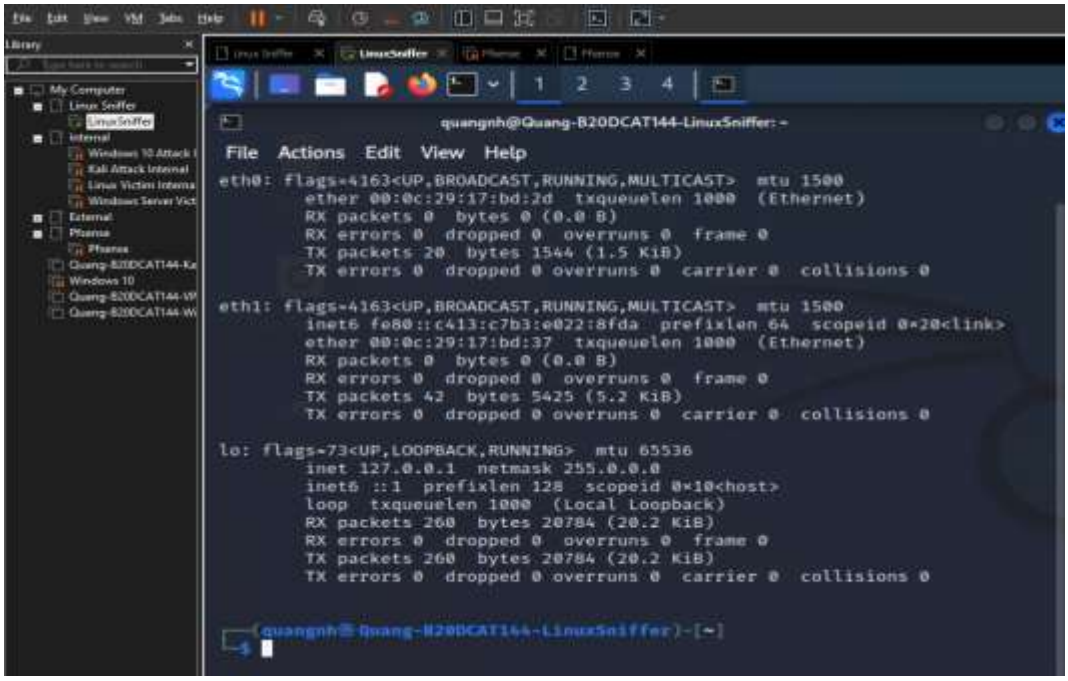
1. Chuẩn bị môi trường

- Phần mềm VMWareWorkStation.
- Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài lab 05 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý:chỉ cần bật các máy cần sử dụng trong bài thực hành.
- Topo mạng như đã cấu hình trong bài 5. Trong bài này chỉ sử dụng các máy trong mạng Internal cho việc sao lưu.



2. Sử dụng tcpdump để bắt gói tin mạng

- Kiểm tra các interfaces trong hệ thống bằng lệnh ifconfig, kết quả trả về đã có 2 interfaces eth0 và eth1



- Linux Sniffer nên hoạt động ở chế độ Promiscuous để nhìn thấy tất cả các lưu lượng mạng. Để tất cả các interface hoạt động ở chế độ Promiscuous, dùng lệnh *ifconfig eth0 –promisc ifconfig eth1 –promisc*

```
ifconfig: `--help' gives usage information.

┌──(root㉿Quang-B20DCAT144-LinuxSniffer)-[~]
└─# sudo ifconfig eth0 promisc

┌──(root㉿Quang-B20DCAT144-LinuxSniffer)-[~]
└─# sudo ifconfig eth1 promisc
```

- Kích hoạt và xác minh interface eth0 bằng lệnh *ifconfig eth0 up ifconfig eth0*

```
┌──(root㉿Quang-B20DCAT144-LinuxSniffer)-[/home/quangnh]
└─# ifconfig eth0 up

┌──(root㉿Quang-B20DCAT144-LinuxSniffer)-[/home/quangnh]
└─# ifconfig eth0
eth0: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        ether 00:0c:29:06:5c:b3  txqueuelen 1000  (Ethernet)
        RX packets 11  bytes 1794 (1.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Tương tự với eth1 *ifconfig eth1 up ifconfig eth1*

```
┌──(root㉿Quang-B20DCAT144-LinuxSniffer)-[/home/quangnh]
└─# ifconfig eth1 up

┌──(root㉿Quang-B20DCAT144-LinuxSniffer)-[/home/quangnh]
└─# ifconfig eth1
eth1: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST>  mtu 1500
        inet 10.10.19.129  netmask 255.255.255.0  broadcast 10.10.19.255
        inet6 fe80::20c:29ff:fe06:5cbd  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:06:5c:bd  txqueuelen 1000  (Ethernet)
        RX packets 12  bytes 1656 (1.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 124  bytes 11709 (11.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Dùng tcpdump –help để xem các option hiện có của tcpdump
- Chạy tcpdump trên phân đoạn mạng mà eth0 được kết nối bằng lệnh

Sudo tcp dump -i eth0 icmp

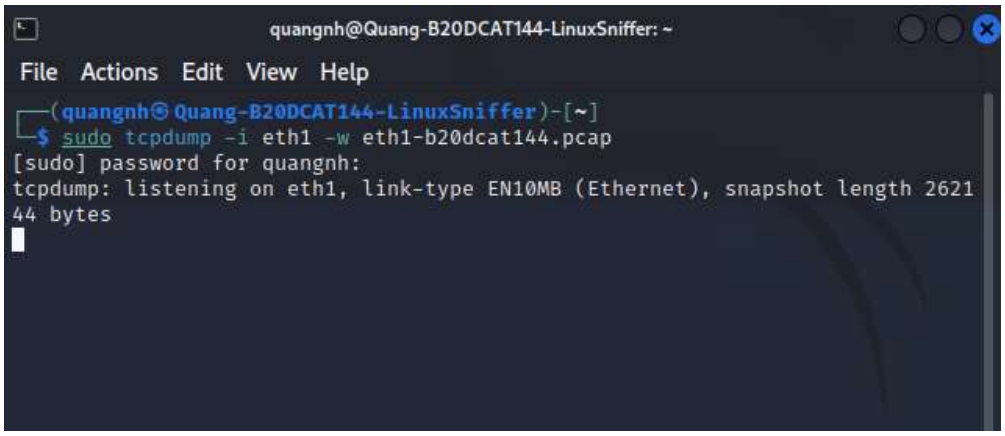
```
┌──(root㉿Quang-B20DCAT144-LinuxSniffer)-[/home/quangnh]
└─# sudo tcpdump -i eth0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:58:53.542004 IP 192.168.100.201 > 192.168.100.5: ICMP echo request, id 1,
seq 18, length 40
```

và gửi vào 1 file (file được đặt tên là eth0-b20dcat144.pcap)

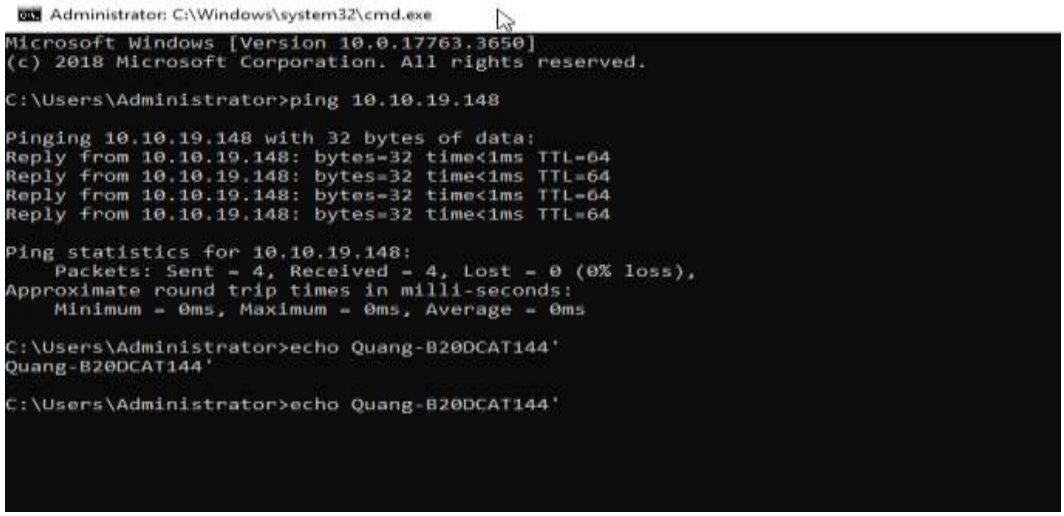
```
root@Quang-B20DCAT144-LinuxSniffer: /home/quangnh
File  Actions  Edit  View  Help
┌──(quangnh㉿Quang-B20DCAT144-LinuxSniffer)-[~]
└─$ sudo su
[sudo] password for quangnh:
┌──(root㉿Quang-B20DCAT144-LinuxSniffer)-[/home/quangnh]
└─# sudo tcpdump -i eth0 -w eth0-b20dcat144.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 2621
44 bytes
```

Tương tự với eth1

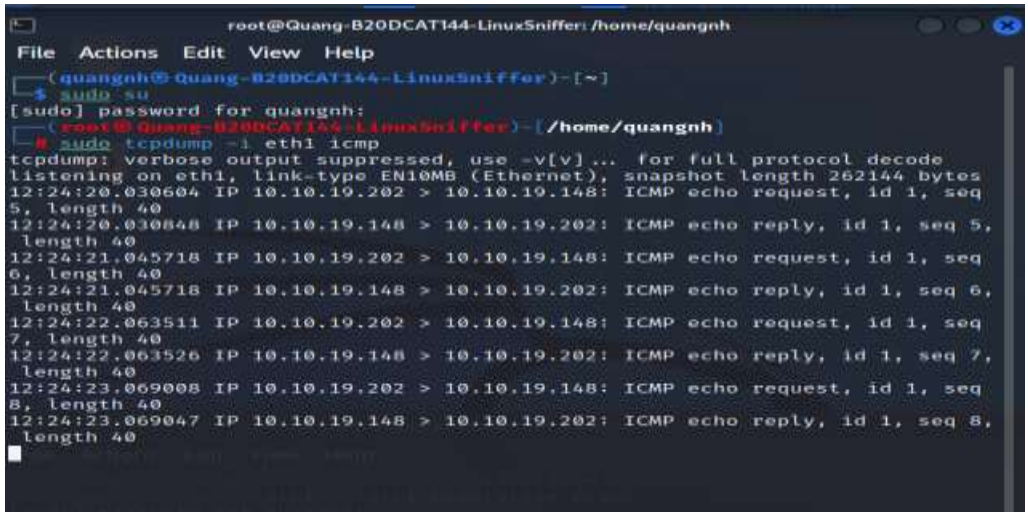
```
┌──(quangnh㉿Quang-B20DCAT144-LinuxSniffer)-[~]
└─$ sudo su
[sudo] password for quangnh:
┌──(root㉿Quang-B20DCAT144-LinuxSniffer)-[/home/quangnh]
└─# sudo tcpdump -i eth1 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

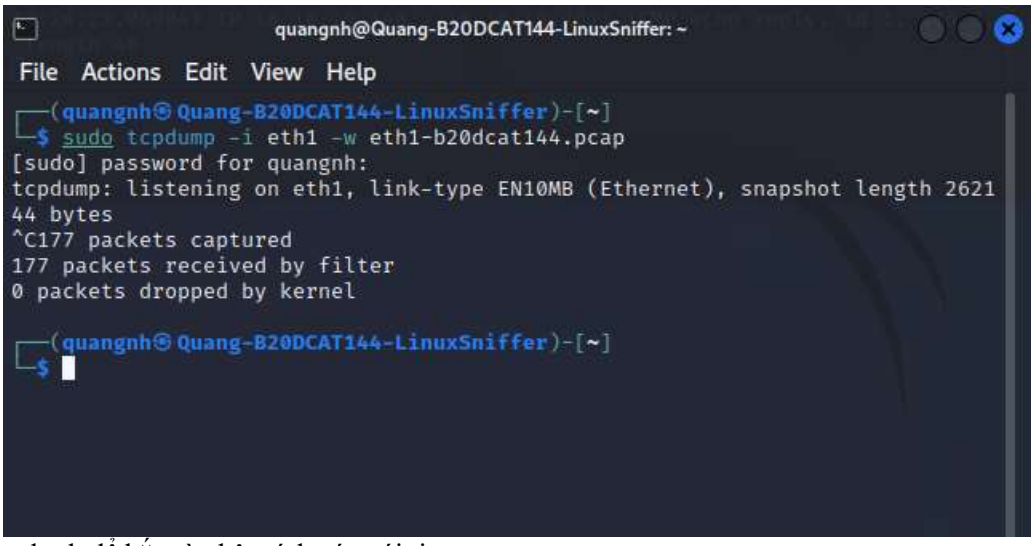


• Từ máy Windows Server Victim External ping đến Kali Attack External



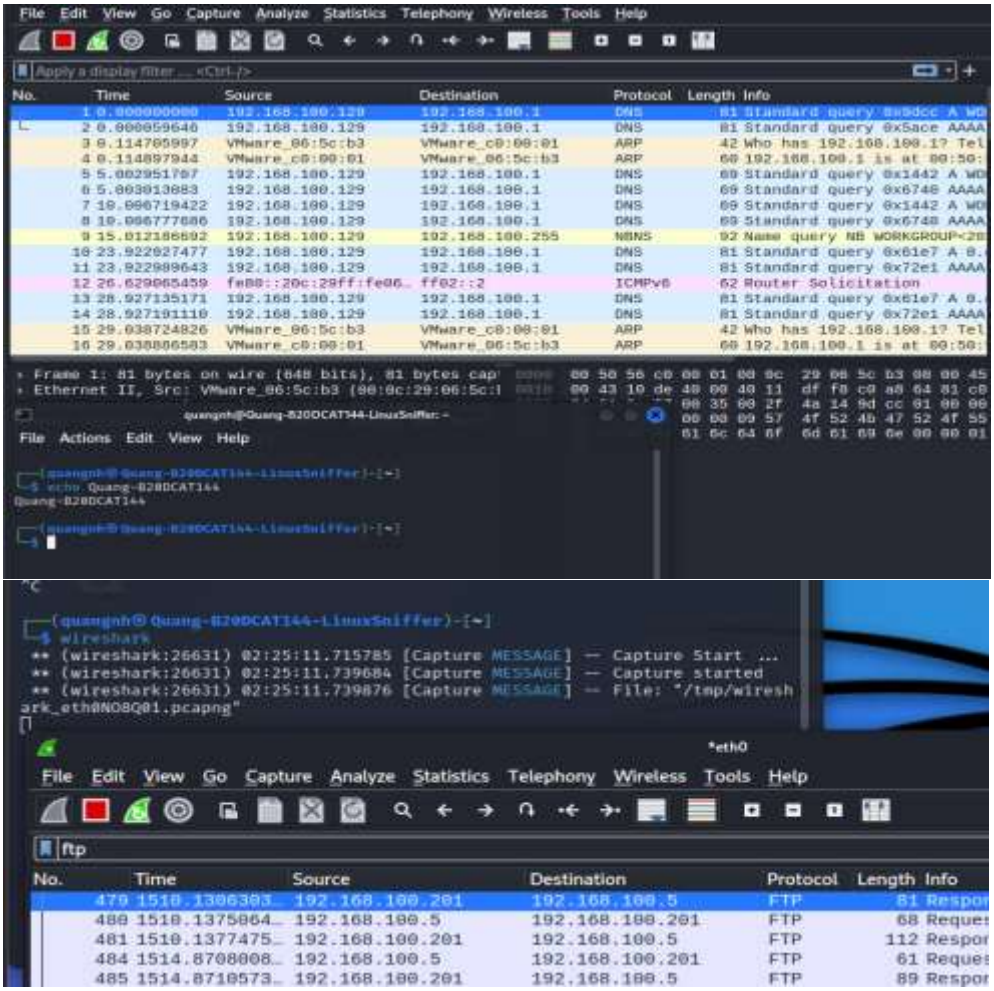
• Từ máy Linux Sniffer bắt được dữ liệu





2.2 Sử dụng Wireshark để bắt và phân tích các gói tin

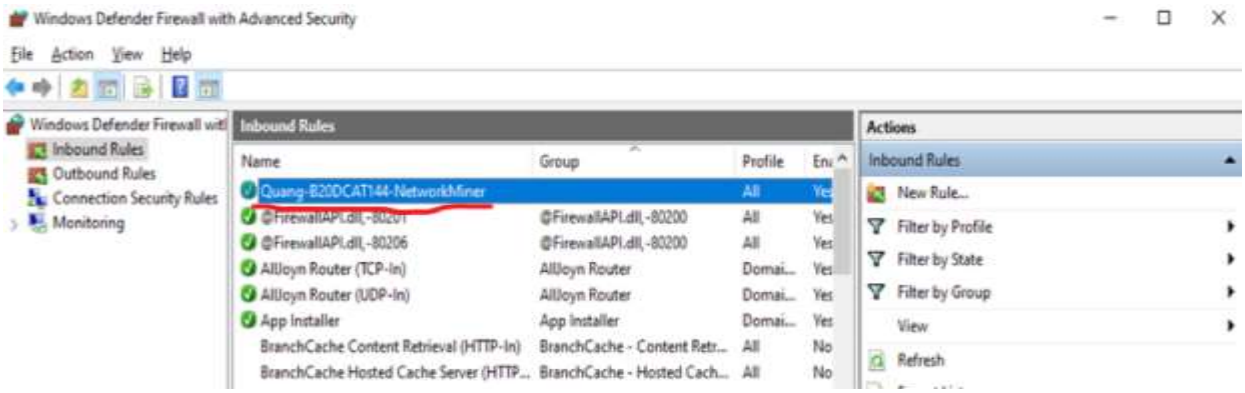
• Khởi động Wireshark chọn Start ở dòng eth0 để bắt các gói tin trên dải mạng 192.168.100.0/24



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

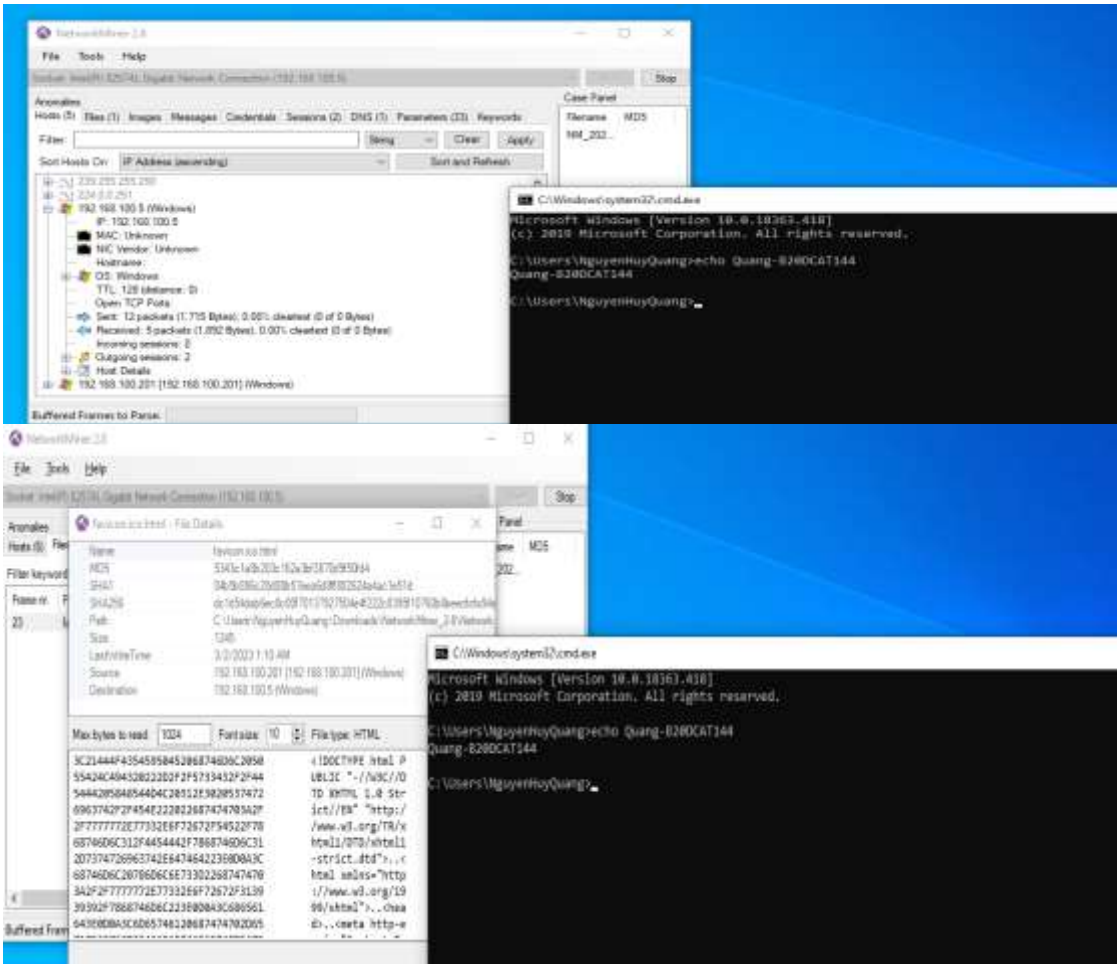
- Trên máy Windows Internal Attack khởi động Network Miner và chọn Socket: Intel® PRO/1000MT Network Connection(192.168.100.5) bắt đầu bắt gói tin

• Tạo Inboud Rule trong Windows Firewall



• Dùng Internet Explorer để kết nối đến trang web của Windows Server Internal Victim http://192.168.100.201

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



3. Tài liệu tham khảo
   - grep: https://linuxcommand.org/lc3_man_pages/grep1.html
   - gawk: http://www.gnu.org/software/gawk/manual/gawk.html
   - find:https://docs.microsoft.com/en-us/windowsserver/administration/windows commands/find
   - xhydra: https://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html