HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BÀI BÁO CÁO THỰC HÀNH SỐ 8

MÔN THỰC TẬP CƠ SỞ

BẮT DỮ LIỆU MẠNG

Tên sinh viên: Ninh Chí Hướng

Mã sinh viên: B20DCAT094

Lớp: D20CQAT02-B

Giảng viên hướng dẫn : Th.s Ninh Thị Thu Trang

HÀ NỘI, THÁNG 5/2023

Table of Contents

I. Tìm hiểu lý thuyết

-TCPDUMP thực chất là công cụ được phát triển nhằm mục đích nhận diện và phân tích các gói dữ liệu mạng theo dòng lệnh.

-TCPDUMP cho phép khách hàng chặn và hiển thị các gói tin được truyền đi hoặc được nhận trên một mạng có sự tham gia của máy tính.

-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.

-Wireshark là một bộ phân tích gói mạng (network packet analyzer). Một network packet analyzer sẽ cố gắng nắm bắt các network packets và cố gắng hiển thị dữ liệu gói đó càng chi tiết càng tốt.

Sử dụng Wireshark nhằm các mục đích sau:

+Network administrators sử dụng Wireshark để khắc phục sự cố mạng.

+Các kỹ sư Network security sử dụng Wireshark để kiểm tra các vấn đề bảo mật.

+Các kỹ sư QA sử dụng Wireshark để xác minh các network applications.

+Các developers sử dụng Wireshark để gỡ lỗi triển khai giao thức.

+Mọi người sử dụng Wireshark để học internals giao thức mạng.

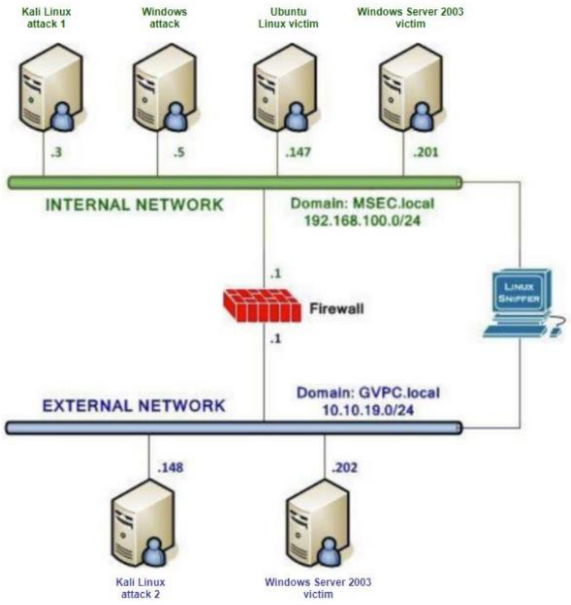
-Cách hoạt động của Wireshark:

1. Bắt gói – Packet Capture
2. Lọc – Filtering
3. Hiển thị trực quan – Visualization

-Network Miner là một công cụ phân tích bảo mật mạng Nguồn Mở di động có thể giám sát lưu lượng của bộ điều hợp mạng được kết nối trong hệ điều hành Windows. Nó sử dụng một công cụ thu thập gói / dò tìm mạng thụ động có thể phát hiện IP, tên máy chủ, hệ điều hành, cổng và nhiều thông tin khác của bất kỳ kết nối nào. Công cụ bảo mật mạng yêu cầu cài đặt - riêng biệt - của WinPcap để hoạt động đúng và đáng tin cậy.

-Mục đích chính của Network Miner là thu thập dữ liệu để phân tích trong tương lai (chẳng hạn như phân tích bằng chứng pháp y) hơn là thu thập dữ liệu liên quan đến lưu lượng trên mạng. Thông tin được nhóm theo máy chủ chứ không phải theo gói hoặc khung mặc dù có thể chuyển đổi chế độ xem dễ dàng trong giao diện phần mềm.

II.Thực hành



Ta cấu hình các máy theo như mô hình bên cạnh .

1. Sử dụng tcpdump

-Đăng nhập Linux Sniffer và xem tất cả các interfaces trong hệ thống (root@bt:~#ifconfig -a), kích hoạt các interfaces(eth0, eth1) hoạt động ở chế độ hỗn hợp, sau đó khởi động tcpdump. Bắt gói tin trên dải mạng 192.168.100.0/24 và gửi vào một file

```
┌──(root㉿B20AT094-NinhChiHuong-kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.19.5  netmask 255.255.255.0  broadcast 10.10.19.255
        inet6 fe80::20c:29ff:fe4d:b329  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:4d:b3:29  txqueuelen 1000  (Ethernet)
        RX packets 139  bytes 10338 (10.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 93  bytes 9172 (8.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.5  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::a026:4864:7523:8aac  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:4d:b3:33  txqueuelen 1000  (Ethernet)
        RX packets 46  bytes 5253 (5.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 88  bytes 12345 (12.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 288  bytes 24312 (23.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 288  bytes 24312 (23.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

ip của 2 interface trên máy kali

```
┌──(root㉿B20AT094-NinhChiHuong-kali)-[~]
└─# ifconfig eth0 -promisc

┌──(root㉿B20AT094-NinhChiHuong-kali)-[~]
└─# ifconfig eth1 -promisc
```

Bật chế độ hỗn hợp

Ip của các máy ở External

```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1da9:7fce:9209:5567%5
   IPv4 Address. . . . . . . . . . . : 10.10.19.202
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\Administrator>echo B20AT094-Ninhchihuong && date
B20AT094-Ninhchihuong
The current date is: Mon 05/08/2023
Enter the new date: (mm-dd-yy)
```

```
C:\Users\Admin>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.19.148
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{EF2B8BF2-C8F5-44A0-9B3C-469C424D5743}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Admin>echo B20AT094-Ninhchihuong && date
B20AT094-Ninhchihuong
The current date is: Mon 05/08/2023
Enter the new date: (mm-dd-yy)
```

IP Các máy ở dải mạng internal

```
C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4598:8ea1:49bb:7a49%10
   IPv4 Address. . . . . . . . . . . : 192.168.100.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Windows\system32>echo B20AT094-Ninhchihuong && date
B20AT094-Ninhchihuong
The current date is: Mon 05/08/2023
Enter the new date: (mm-dd-yy)
```

```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f427:7250:12b9:dbcd%5
   IPv4 Address. . . . . . . . . . . : 192.168.100.201
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\Administrator>echo B20AT094-Ninhchihuong && date
B20AT094-Ninhchihuong
The current date is: Mon 05/08/2023
Enter the new date: (mm-dd-yy)
```

Bây giờ ta sẽ cho các máy ở cùng dải mạng ping với nhau , sau đó máy linux sniffer sẽ lắng nghe gói tin ICMP

```
C:\Users\Admin>ping 10.10.19.202

Pinging 10.10.19.202 with 32 bytes of data:
Reply from 10.10.19.202: bytes=32 time<1ms TTL=128
Reply from 10.10.19.202: bytes=32 time=2ms TTL=128
Reply from 10.10.19.202: bytes=32 time<1ms TTL=128
Reply from 10.10.19.202: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.19.202:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\Admin>echo B20AT094-Ninhchihuong && date
B20AT094-Ninhchihuong
The current date is: Mon 05/08/2023
Enter the new date: (mm-dd-yy)
```

```
C:\Users\Administrator>ping 192.168.100.3

Pinging 192.168.100.3 with 32 bytes of data:
Reply from 192.168.100.3: bytes=32 time<1ms TTL=128
Reply from 192.168.100.3: bytes=32 time<1ms TTL=128
Reply from 192.168.100.3: bytes=32 time<1ms TTL=128
Reply from 192.168.100.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.100.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>echo B20AT094-Ninhchihuong && date
B20AT094-Ninhchihuong
The current date is: Mon 05/08/2023
Enter the new date: (mm-dd-yy)
```

Chạy lệnh tcpdump -I eth0 icmp để hiện gói tin icmp

```
┌──(root㉿B20AT094-NinhChiHuong-kali)-[~]
└─# 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
11:57:51.012046 IP 10.10.19.148 > 10.10.19.202: ICMP echo request, id 1, seq 5, length 40
11:57:51.012167 IP 10.10.19.202 > 10.10.19.148: ICMP echo reply, id 1, seq 5, length 40
11:57:52.025427 IP 10.10.19.148 > 10.10.19.202: ICMP echo request, id 1, seq 6, length 40
11:57:52.027329 IP 10.10.19.202 > 10.10.19.148: ICMP echo reply, id 1, seq 6, length 40
11:57:53.023561 IP 10.10.19.148 > 10.10.19.202: ICMP echo request, id 1, seq 7, length 40
11:57:53.023679 IP 10.10.19.202 > 10.10.19.148: ICMP echo reply, id 1, seq 7, length 40
11:57:54.038019 IP 10.10.19.148 > 10.10.19.202: ICMP echo request, id 1, seq 8, length 40
11:57:54.038175 IP 10.10.19.202 > 10.10.19.148: ICMP echo reply, id 1, seq 8, length 40
```

Tương tự với cổng eth1

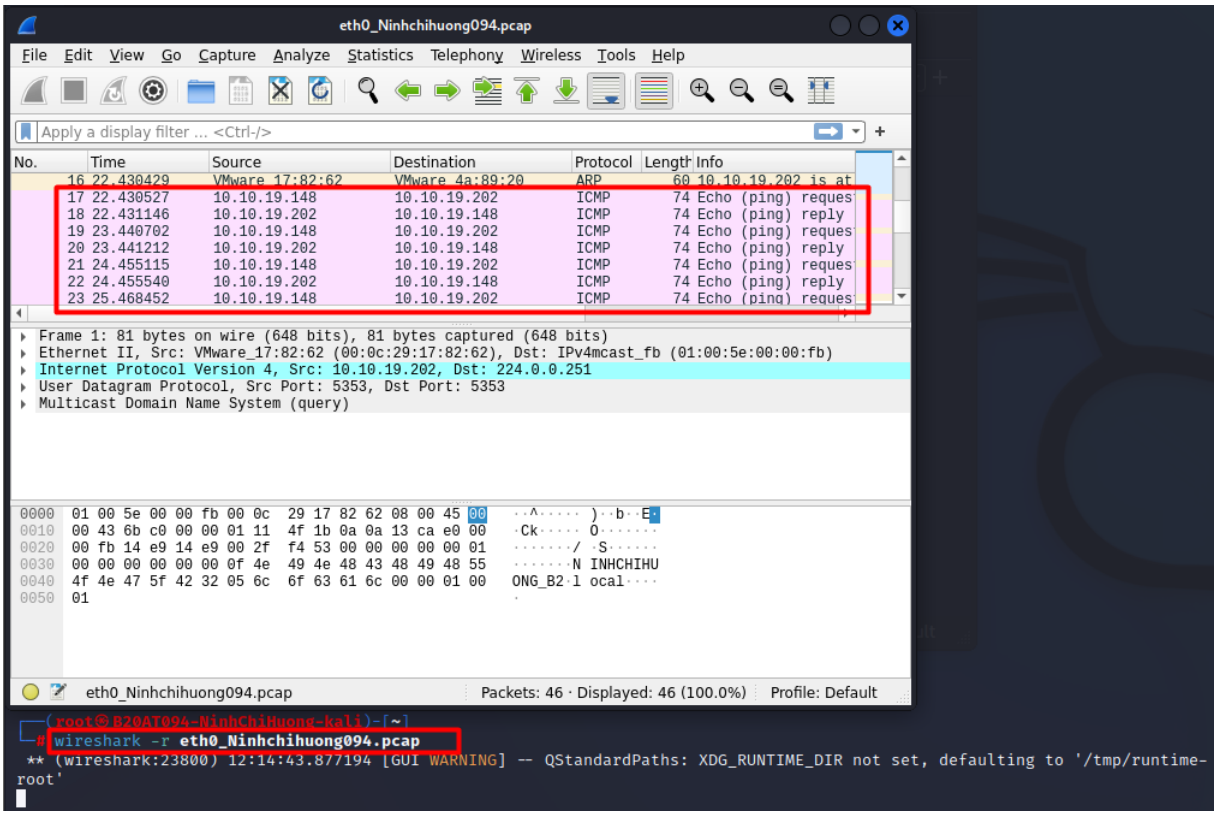
```
┌──(root㉿B20AT094-NinhChiHuong-kali)-[~]
└─# tcpdump -i eth1 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:56:18.374561 IP 192.168.100.201 > 192.168.100.3: ICMP echo request, id 1, seq 398, length 40
11:56:18.374992 IP 192.168.100.3 > 192.168.100.201: ICMP echo reply, id 1, seq 398, length 40
11:56:19.380568 IP 192.168.100.201 > 192.168.100.3: ICMP echo request, id 1, seq 399, length 40
11:56:19.380779 IP 192.168.100.3 > 192.168.100.201: ICMP echo reply, id 1, seq 399, length 40
11:56:20.386084 IP 192.168.100.201 > 192.168.100.3: ICMP echo request, id 1, seq 400, length 40
11:56:20.386267 IP 192.168.100.3 > 192.168.100.201: ICMP echo reply, id 1, seq 400, length 40
11:56:21.391737 IP 192.168.100.201 > 192.168.100.3: ICMP echo request, id 1, seq 401, length 40
11:56:21.391911 IP 192.168.100.3 > 192.168.100.201: ICMP echo reply, id 1, seq 401, length 40
```

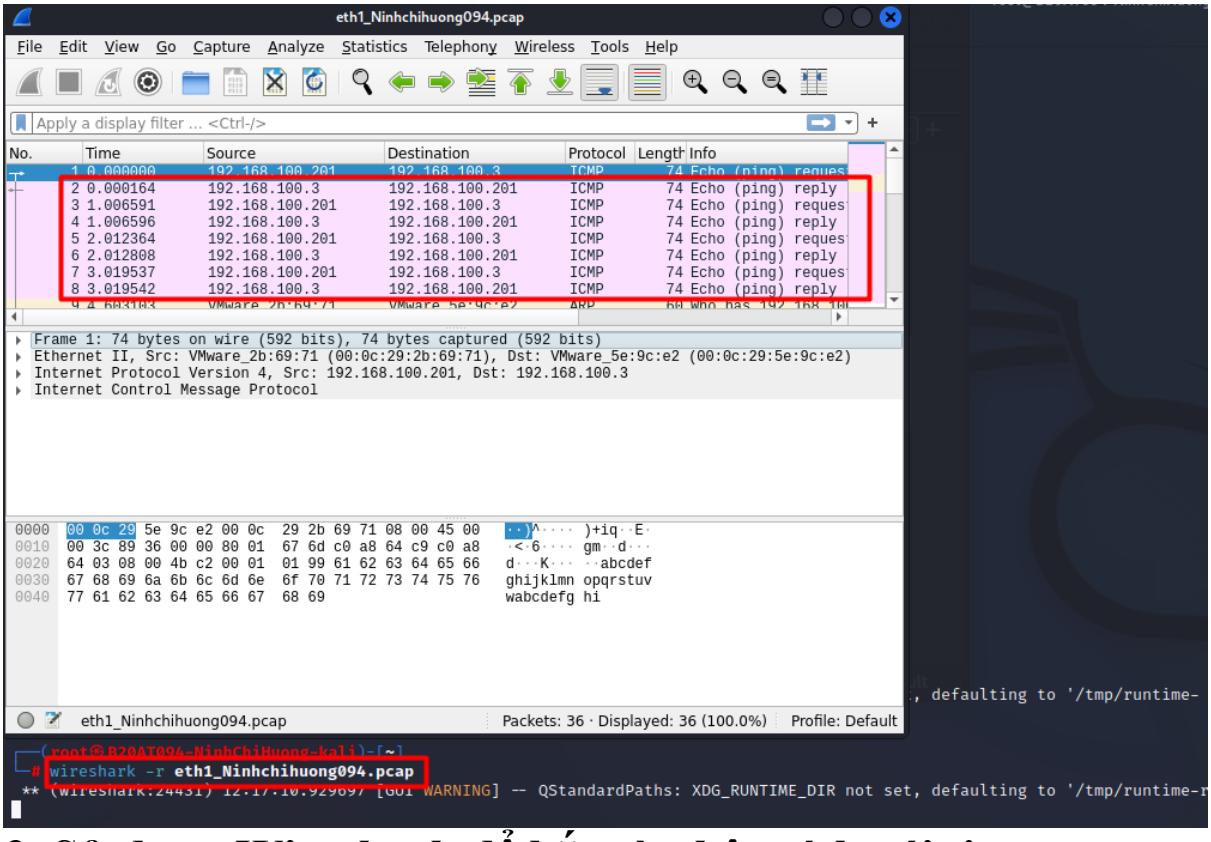
Bây giờ ta lưu vào 2 file eth0_ninhchihuong094.pcap và eth1_ninhchihuong094.pcap

```
┌──(root㉿B20AT094-NinhChiHuong-kali)-[~]
└─# tcpdump -i eth0 -w eth0_Ninhchihuong094.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C46 packets captured
46 packets received by filter
0 packets dropped by kernel

┌──(root㉿B20AT094-NinhChiHuong-kali)-[~]
└─# tcpdump -i eth1 -w eth1_Ninhchihuong094.pcap
tcpdump: listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C36 packets captured
36 packets received by filter
0 packets dropped by kernel
```

Dùng wireshark để xem file vừa lưu bằng cách chạy lệnh :
Wireshark -r eth0_Ninhchihuong094.pcap
Wireshark -r eth1_Ninhchihuong094.pcap

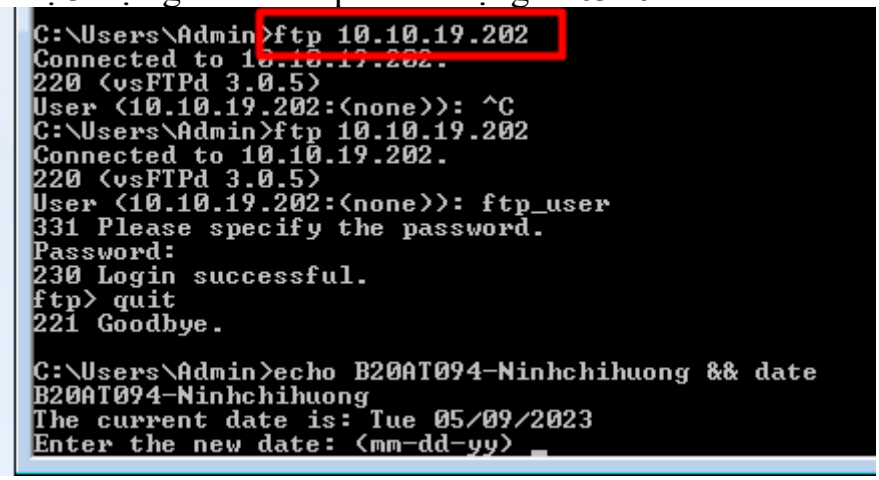




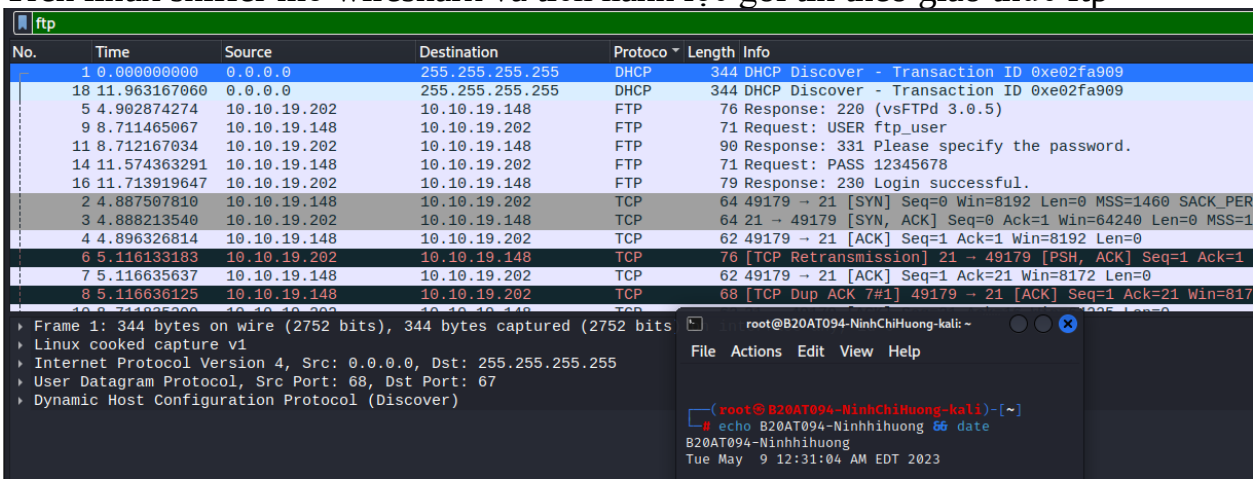
2. Sử dụng Wireshark để bắt và phân tích gói tin

Trên máy Linux Sniffer, bật các interfaces eth0, eth1 và khởi động Wireshark. Trong Capture Interfaces chọn Start ở dòng eth0 để bắt gói tin trên dải mạng 192.168.100.0 Địa chỉ ip máy windows server

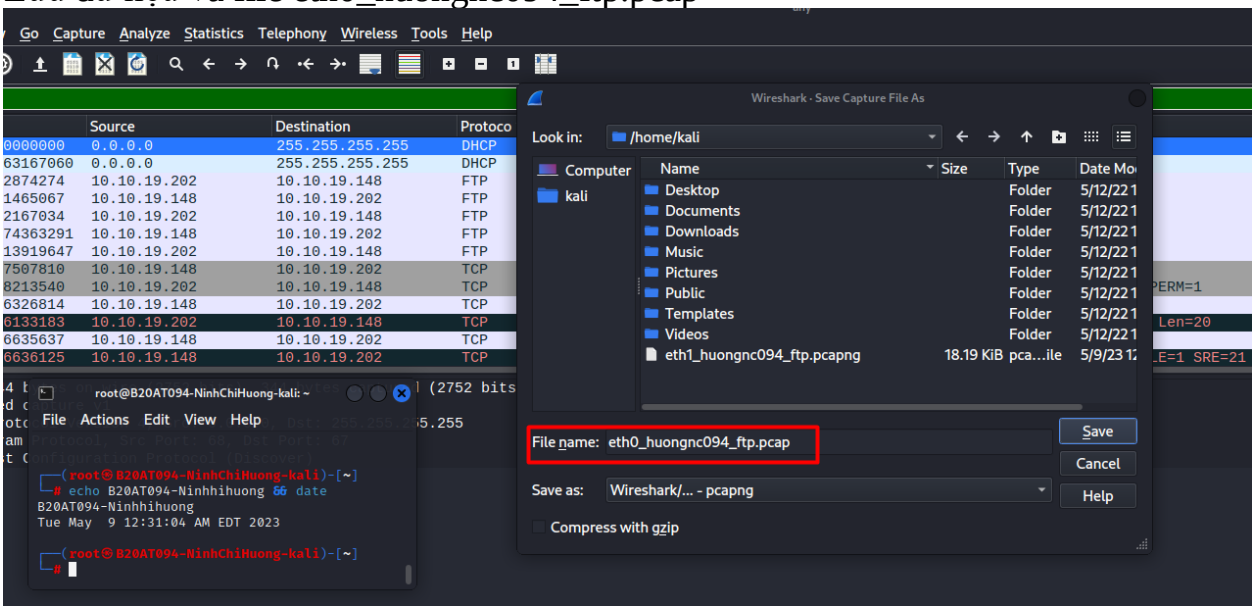
Thực hiện giao thức ftp ở dải mạng External



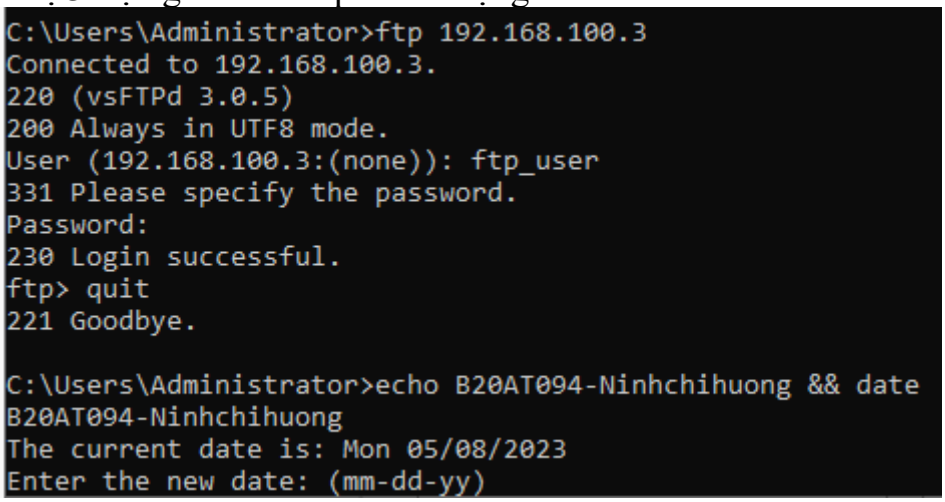
Trên linux sniffer mở wireshark và tiến hành lọc gói tin theo giao thức ftp



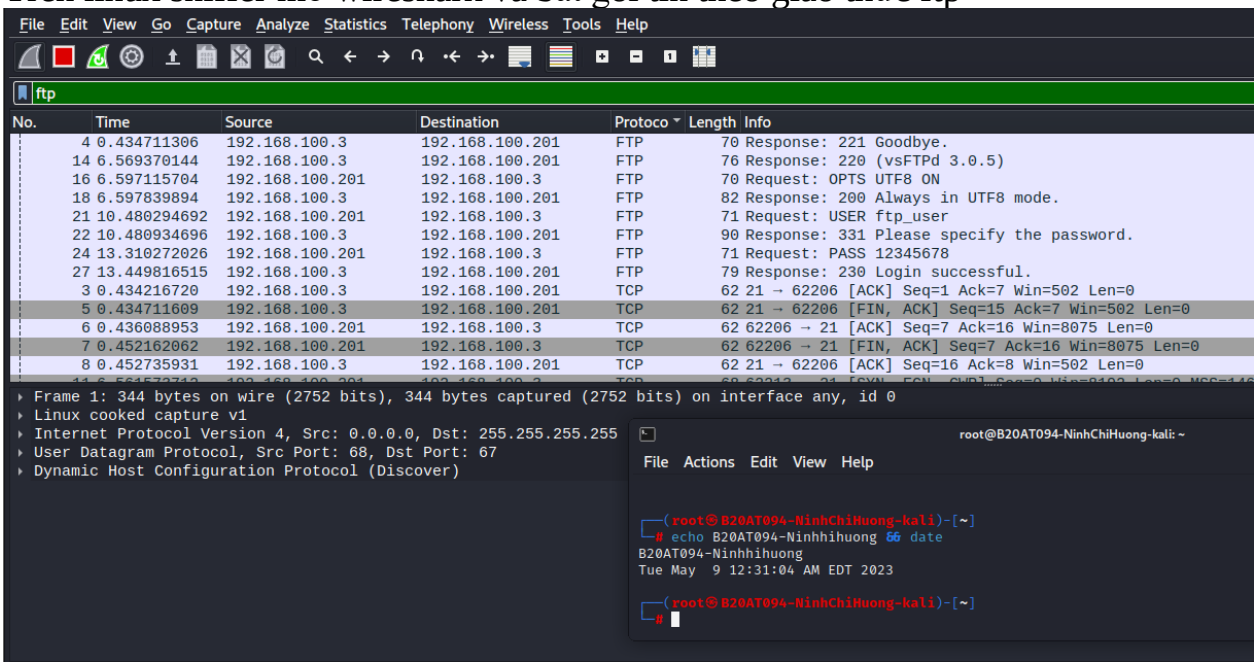
Lưu dữ liệu và file eth0_huongnc094_ftp.pcap



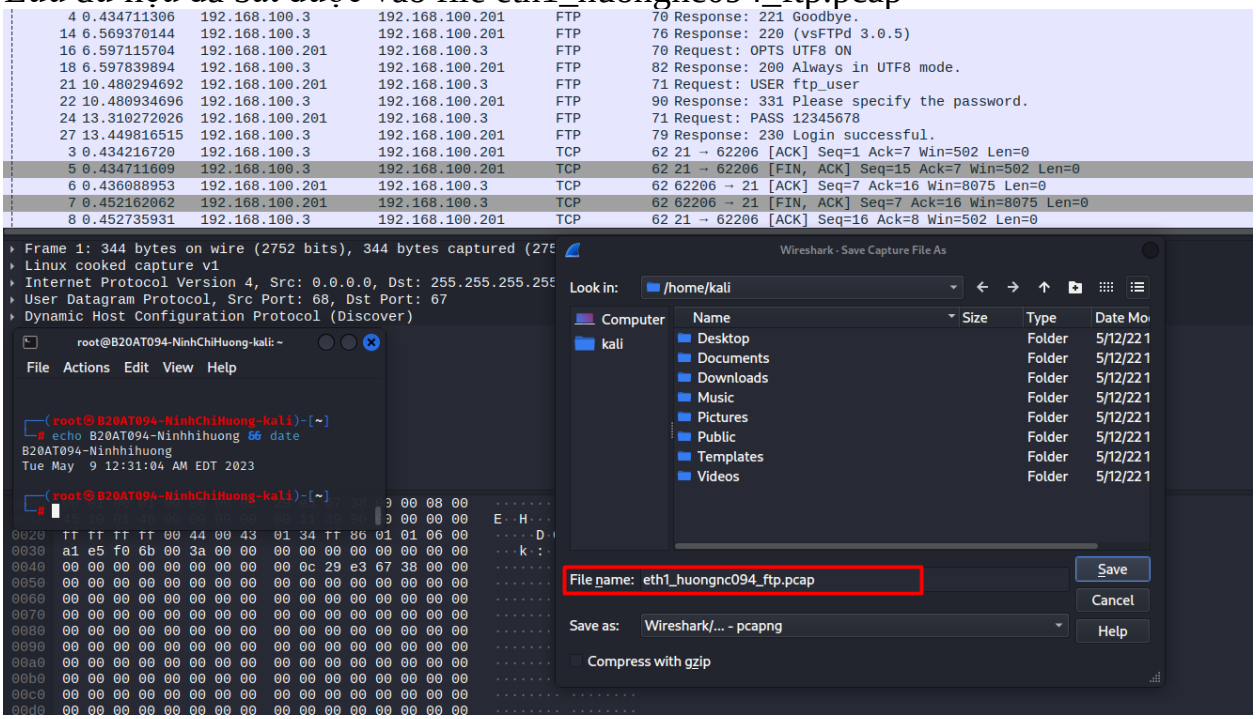
Thực hiện giao thức ftp ở dải mạng internal



Trên linux sniffer mở wireshark và bắt gói tin theo giao thức ftp

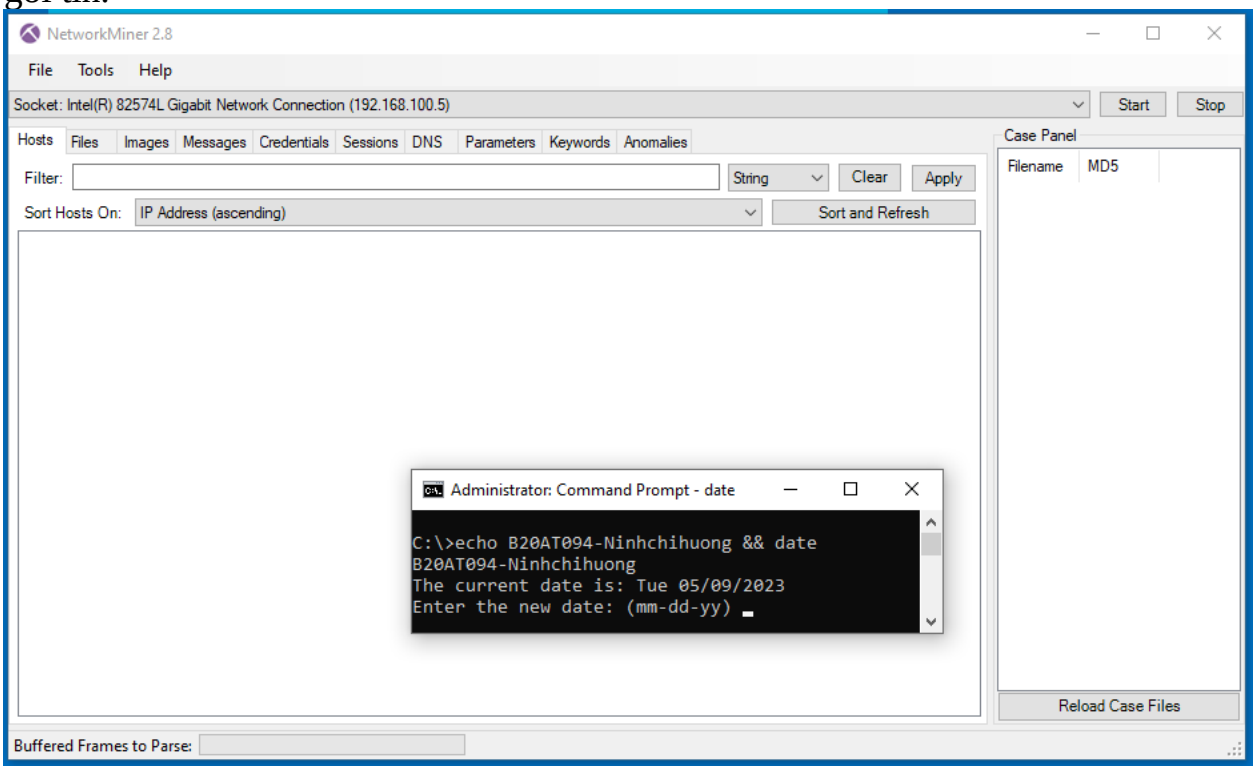


Lưu dữ liệu đã bắt được vào file eth1_huongnc094_ftp.pcap

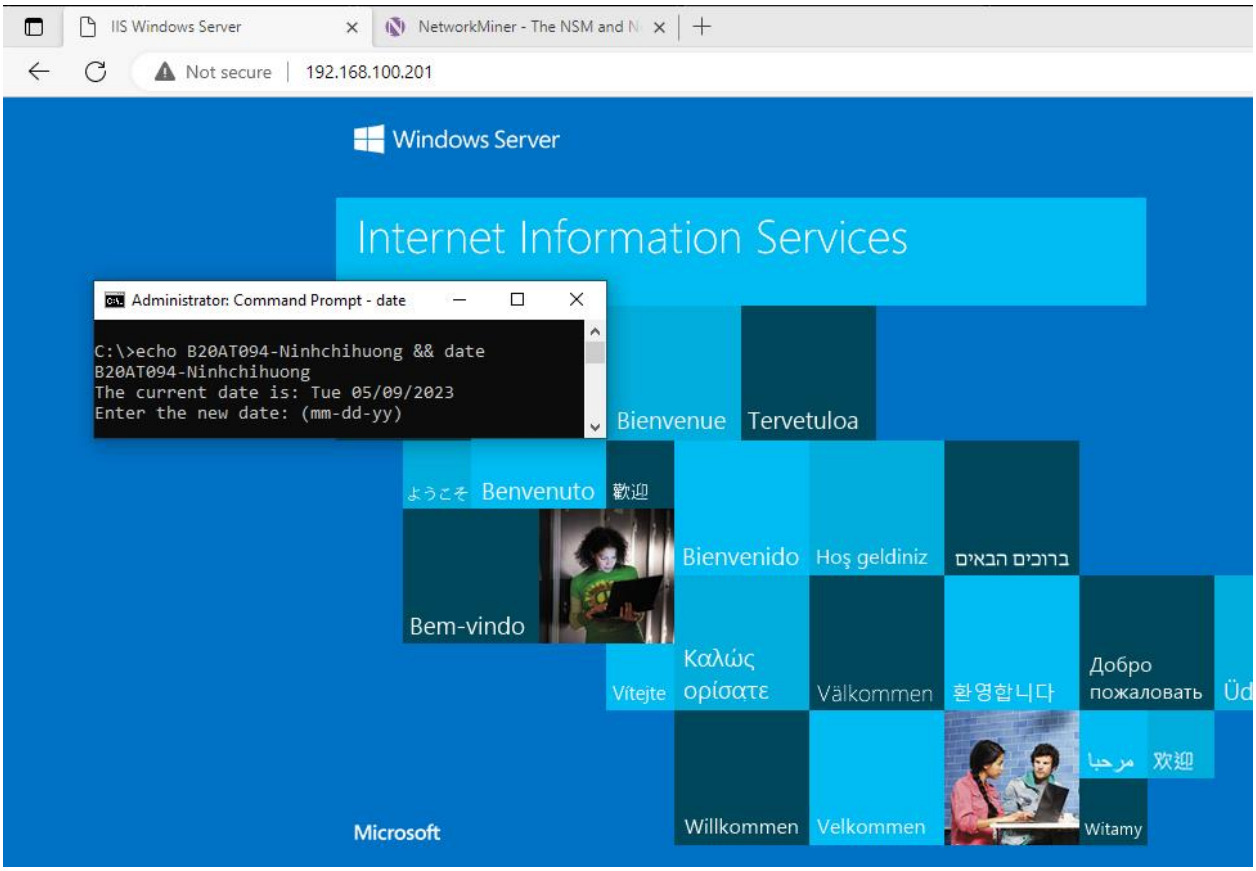


3. Sử dụng Network Miner để bắt và phân tích các gói tin

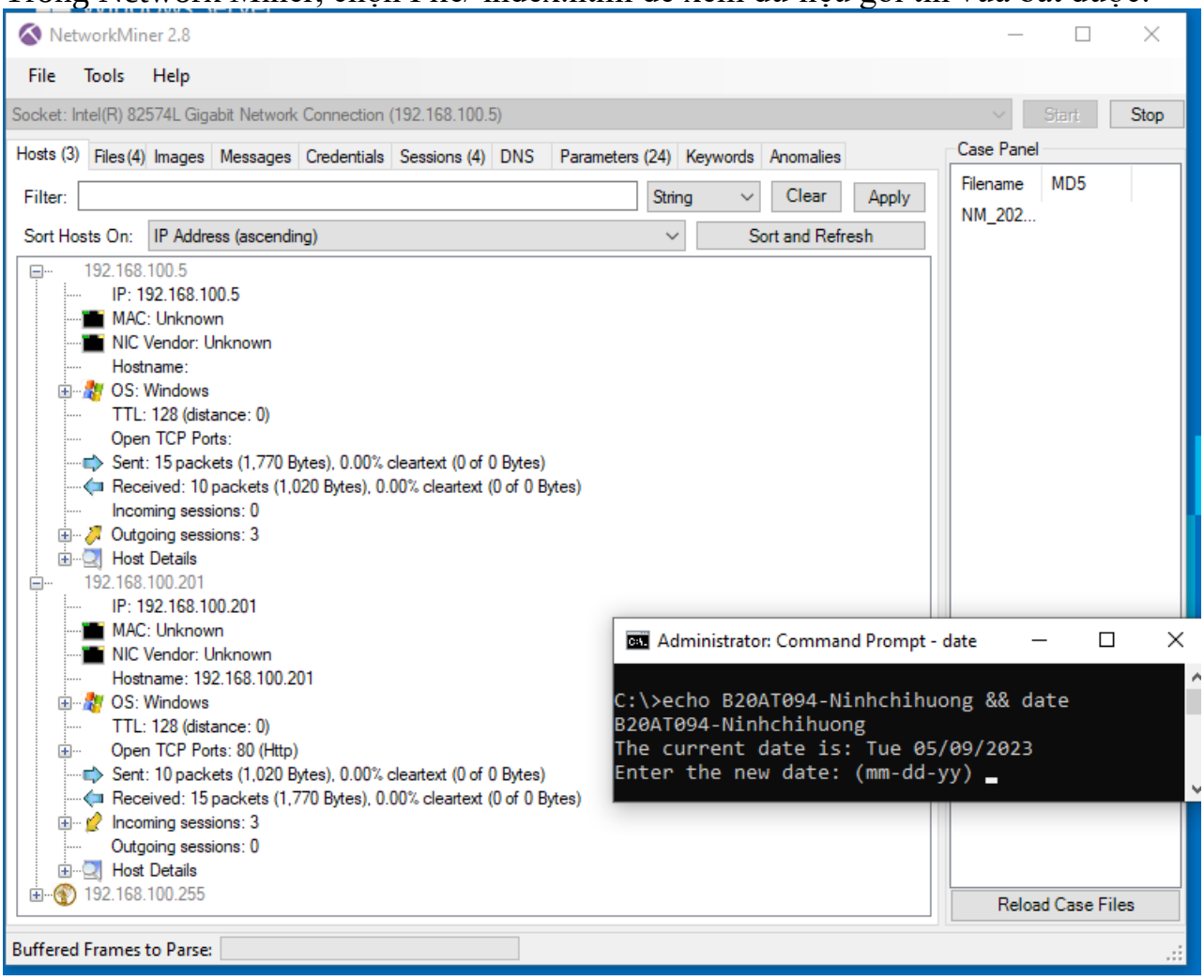
Trên máy windows 10 internal attack khởi động network miner và chọn Socket: Intel® PRO/1000MT Network Connection(192.168.100.5) và bắt đầu bắt gói tin.

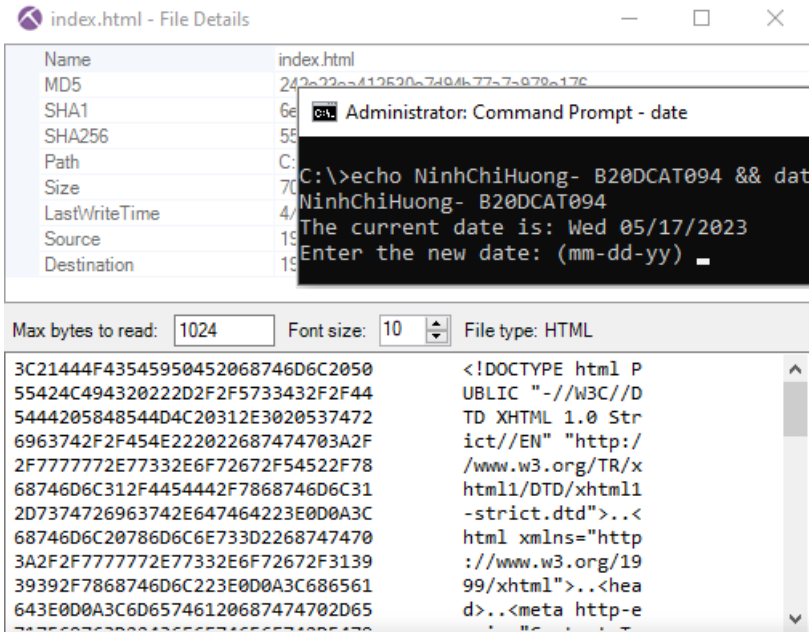


Sử dụng Internet Explorer để kết nối đến trang web của Windows 2003 Server Internal Victim: http://192.168.100.201/. Sau đó dừng quá trình bắt gói tin.



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





III. Tài liệu tham khảo

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