HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 1

BÀI THỰC HÀNH 8

THỰC TẬP CƠ SỞ

Họ và tên : Đinh Quang Hiếu

Mã sinh viên: B19DCAT065

Giảng viên giảng dạy: Hoàng Xuân Dậu

HÀ NỘI, THÁNG 4/2022

Bài 8: Bắt dữ liệu mạng

I. Giới thiệu chung

1. Mục đích

• Tìm Sử dụng tcpdump để bắt gói tin mạng

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

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

2. Yêu cầu

• Tìm hiểu lý thuyết o 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 người dùng hiển thị TCP/IP và các gói khác đang được truyền hoặc nhận qua mạng mà máy tính được gắn vào.

▪ Tcpdump hoạt động trên hầu hết các hệ điều hành Unix : Linux , Solaris , FreeBSD,… o Wireshark

▪ Là một ứng dụng dùng để bắt (capture), phân tích và xác định các vấn đề liên quan đến network như: rớt gói tin, kết nối chậm, hoặc các truy cập bất thường.

▪ Cho phép bắt các packet trong thời gian thực (realtime), lưu trữ chúng lại và phân tích offline. Ngoài ra, nó bao gồm các tính năng filter, color coding,...

▪ Có thể sử dụng trên Linux, MacOS và Windows o Network Miner

▪ Là một công cụ phân tích pháp y mạng (NFAT) mã nguồn mở

▪ Có thể phân tích cú pháp tệp PCAP để phân tích ngoại tuyến và tái tạo/tập hợp lại các tệp PCAP.

▪ Dễ dàng thực hiện phân tích lưu lượng mạng nâng cao bằng cách cung cấp các tạo tác được trích xuất trong giao diện người dùng trực quan.

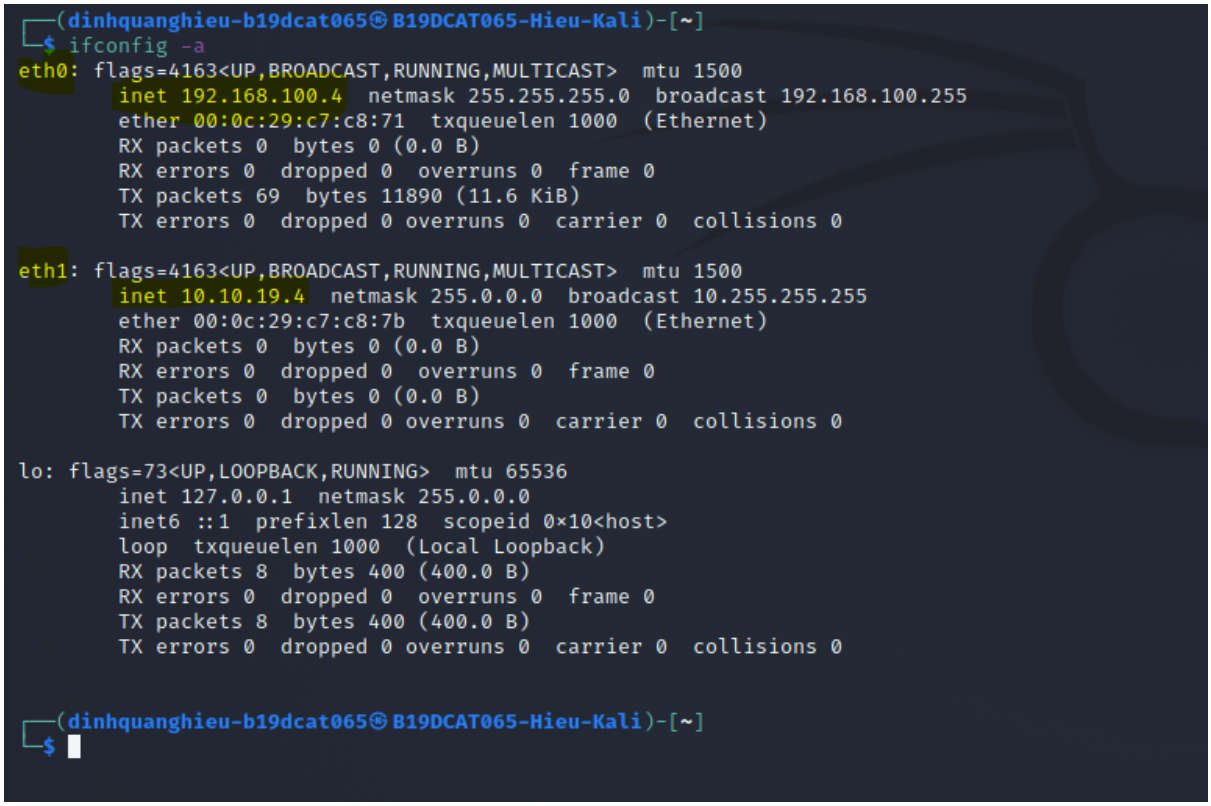
• Chuẩn bị o Phần mềm VMWare Workstation o File máy ảo VMware và hệ thống mạng đã cài đặt trong bài lab 5 o Topo mạng như đã cấu hình trong bài 5

3. Các bước thực hiện

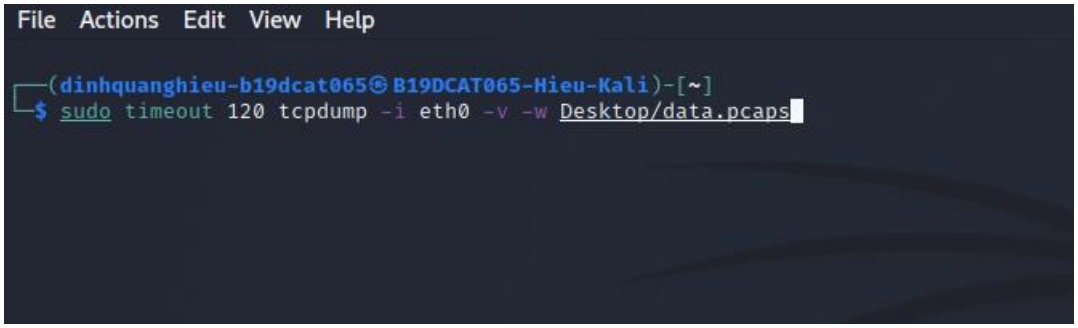
-Sử dụng tcpdump

a) Các bước thực hiện

o 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.



- 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 2 phút)



- Đăng nhập Window Server 2003 và tiến hành ping đến dải mạng internal và dải mạng external.

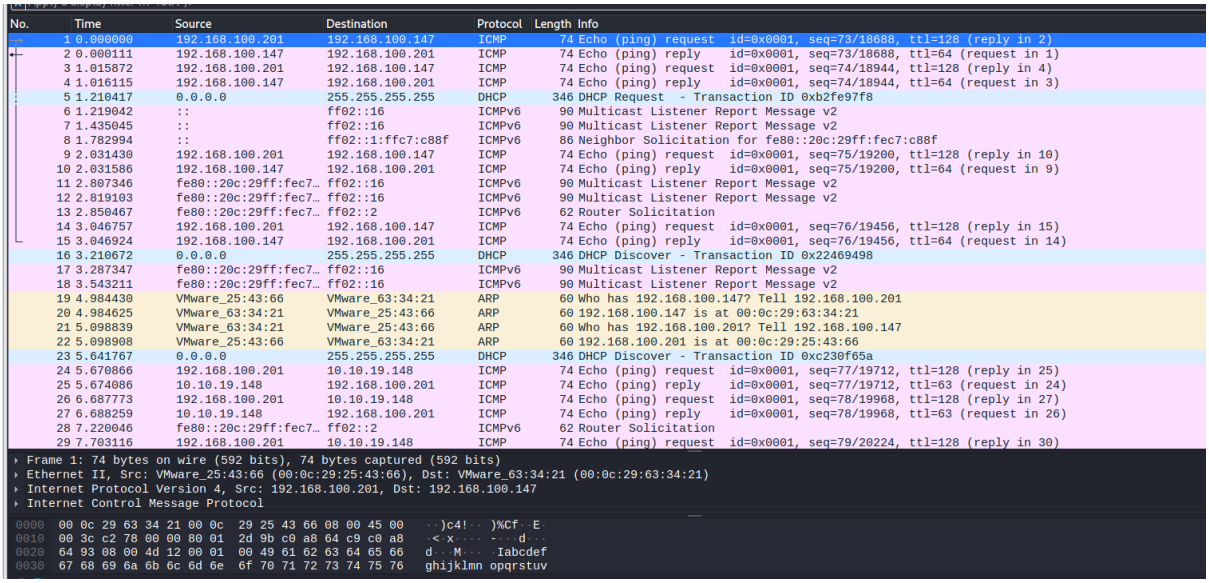
```
C:\Users\Administrator>ping 192.168.100.147

Pinging 192.168.100.147 with 32 bytes of data:
Reply from 192.168.100.147: bytes=32 time<1ms TTL=64
Reply from 192.168.100.147: bytes=32 time<1ms TTL=64
Reply from 192.168.100.147: bytes=32 time<1ms TTL=64
Reply from 192.168.100.147: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.100.147:
    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>ping 10.10.19.148

Pinging 10.10.19.148 with 32 bytes of data:
Reply from 10.10.19.148: bytes=32 time<1ms TTL=63
Reply from 10.10.19.148: bytes=32 time<1ms TTL=63
Reply from 10.10.19.148: bytes=32 time<1ms TTL=63
Reply from 10.10.19.148: bytes=32 time<1ms TTL=63

Ping statistics for 10.10.19.148:
    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 dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065

C:\Users\Administrator>
```

- Trên máy Linux Sniffer, tiến hành bắt gói tin bằng tcpdump, và lưu dữ liệu vào file pcap

```
File  Actions  Edit  View  Help

┌──(dinhquanghieu-b19dcat065㉿B19DCAT065-Hieu-Kali)-[~]
└─$ sudo timeout 120 tcpdump -i eth0 -v -w Desktop/data.pcaps
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
44 packets captured
44 packets received by filter
0 packets dropped by kernel

┌──(dinhquanghieu-b19dcat065㉿B19DCAT065-Hieu-Kali)-[~]
└─$
```

b) Kết quả cần đạt được

o Thu được kết quả bắt gói tin và các file pcap thông qua tcpdump



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.201	192.168.100.147	ICMP	74	Echo (ping) request id=0x0001, seq=73/18688, ttl=128 (reply in 2)
2	0.000111	192.168.100.147	192.168.100.201	ICMP	74	Echo (ping) reply id=0x0001, seq=73/18688, ttl=64 (request in 1)
3	1.015872	192.168.100.201	192.168.100.147	ICMP	74	Echo (ping) request id=0x0001, seq=74/18944, ttl=128 (reply in 4)
4	1.016115	192.168.100.147	192.168.100.201	ICMP	74	Echo (ping) reply id=0x0001, seq=74/18944, ttl=64 (request in 3)
5	1.210417	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0xb2fe97f8
6	1.219042	::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
7	1.435045	::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
8	1.782994	::	ff02::1:ffc7:c88f	ICMPv6	86	Neighbor Solicitation for fe80::20c:29ff:fec7:c88f
9	2.031430	192.168.100.201	192.168.100.147	ICMP	74	Echo (ping) request id=0x0001, seq=75/19200, ttl=128 (reply in 10)
10	2.031586	192.168.100.147	192.168.100.201	ICMP	74	Echo (ping) reply id=0x0001, seq=75/19200, ttl=64 (request in 9)
11	2.807346	fe80::20c:29ff:fec7…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
12	2.819103	fe80::20c:29ff:fec7…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
13	2.850467	fe80::20c:29ff:fec7…	ff02::2	ICMPv6	62	Router Solicitation
14	3.046757	192.168.100.201	192.168.100.147	ICMP	74	Echo (ping) request id=0x0001, seq=76/19456, ttl=128 (reply in 15)
15	3.046924	192.168.100.147	192.168.100.201	ICMP	74	Echo (ping) reply id=0x0001, seq=76/19456, ttl=64 (request in 14)
16	3.210672	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x22469498
17	3.287347	fe80::20c:29ff:fec7…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
18	3.543211	fe80::20c:29ff:fec7…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
19	4.984430	VMware_25:43:66	VMware_63:34:21	ARP	60	Who has 192.168.100.147? Tell 192.168.100.201
20	4.984625	VMware_63:34:21	VMware_25:43:66	ARP	60	192.168.100.147 is at 00:0c:29:63:34:21
21	5.098839	VMware_63:34:21	VMware_25:43:66	ARP	60	Who has 192.168.100.201? Tell 192.168.100.147
22	5.098908	VMware_25:43:66	VMware_63:34:21	ARP	60	192.168.100.201 is at 00:0c:29:25:43:66
23	5.641767	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0xc230f65a
24	5.670866	192.168.100.201	10.10.19.148	ICMP	74	Echo (ping) request id=0x0001, seq=77/19712, ttl=128 (reply in 25)
25	5.674086	10.10.19.148	192.168.100.201	ICMP	74	Echo (ping) reply id=0x0001, seq=77/19712, ttl=63 (request in 24)
26	6.687773	192.168.100.201	10.10.19.148	ICMP	74	Echo (ping) request id=0x0001, seq=78/19968, ttl=128 (reply in 27)
27	6.688259	10.10.19.148	192.168.100.201	ICMP	74	Echo (ping) reply id=0x0001, seq=78/19968, ttl=63 (request in 26)
28	7.220046	fe80::20c:29ff:fec7…	ff02::2	ICMPv6	62	Router Solicitation
29	7.703116	192.168.100.201	10.10.19.148	ICMP	74	Echo (ping) request id=0x0001, seq=79/20224, ttl=128 (reply in 30)

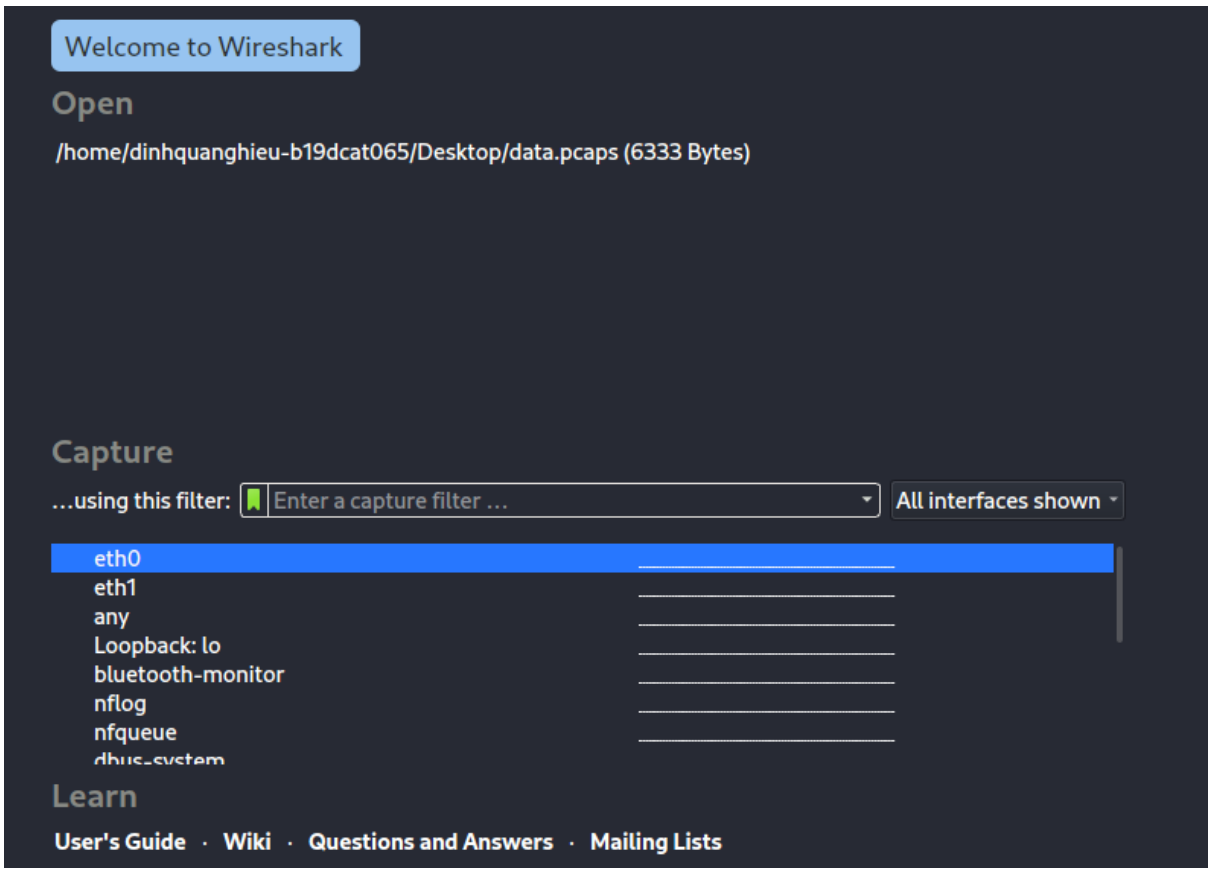
```
▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▸ Ethernet II, Src: VMware_25:43:66 (00:0c:29:25:43:66), Dst: VMware_63:34:21 (00:0c:29:63:34:21)
▸ Internet Protocol Version 4, Src: 192.168.100.201, Dst: 192.168.100.147
▸ Internet Control Message Protocol

0000  00 0c 29 63 34 21 00 0c  29 25 43 66 08 00 45 00   ··)c4!·· )%Cf··E·
0010  00 3c c2 78 00 00 80 01  2d 9b c0 a8 64 c9 c0 a8   ·<·x···· -···d···
0020  64 93 08 00 4d 12 00 01  00 49 61 62 63 64 65 66   d···M···· ·Iabcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
```

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

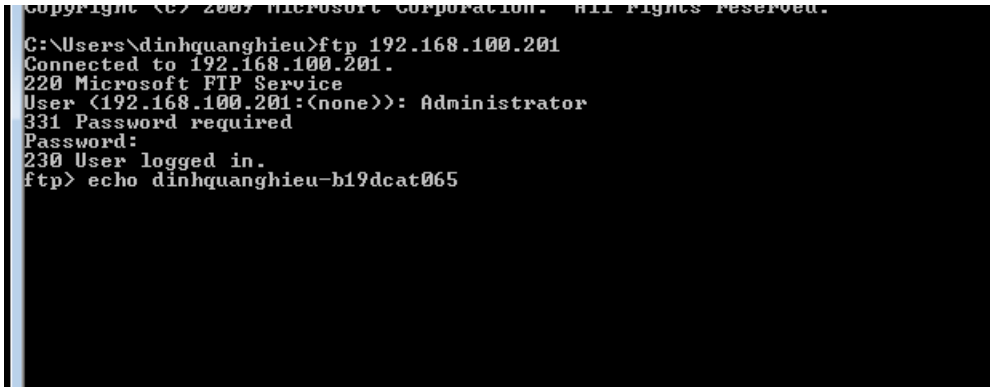
a) Các bước thực hiện

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

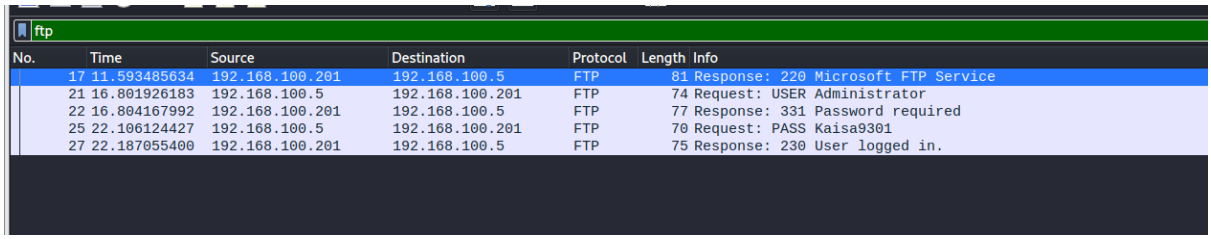
o Trên máy Linux Sniffer, bật các interfaces eth0, eth1 và khởi động Wireshark. Trong Capture Interfaces chọn Start ở dòng eth0 để bắt gói tin trên dải mạng 192.168.100.0



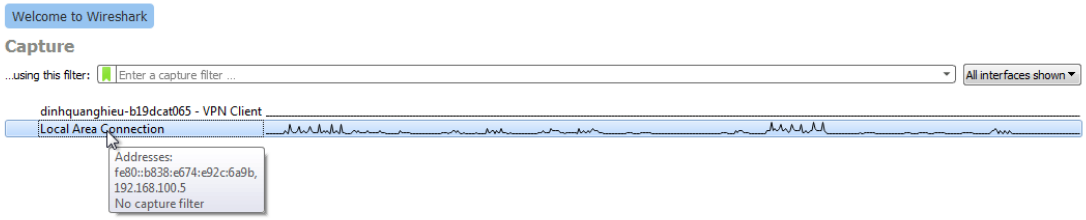
- Trên máy Windows 7 Attack kết nối tới ftp server (C:\ftp 192.168.100.201) trên máy Window Server Internal Victim



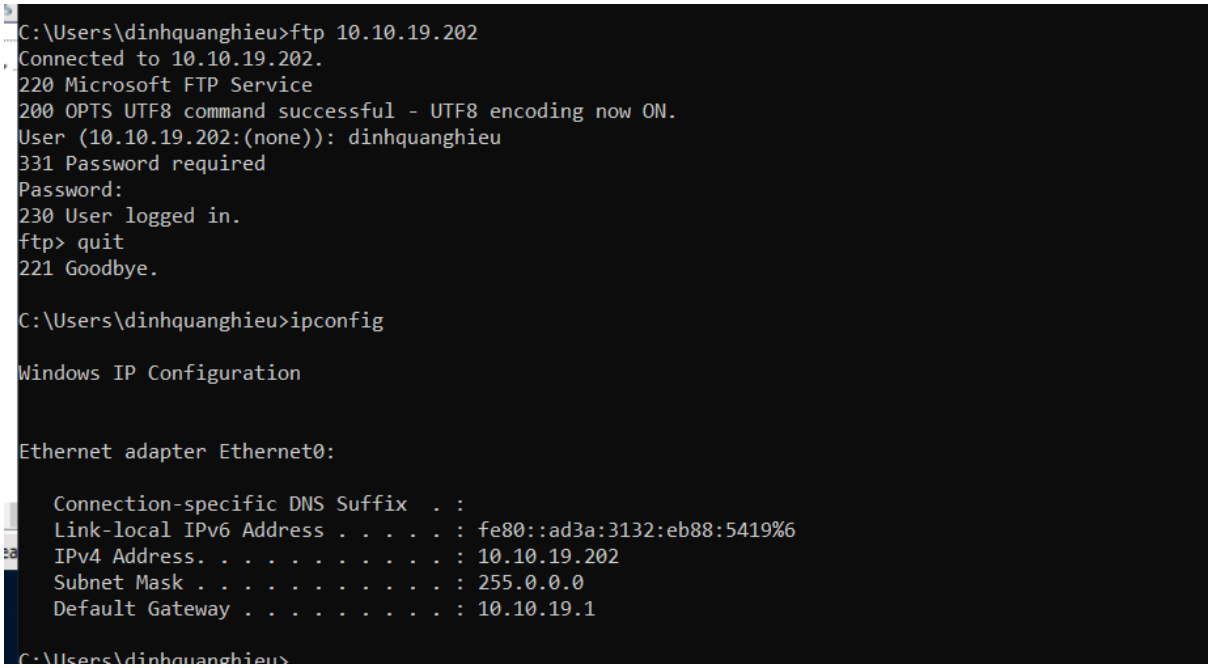
- Trên Linux Sniffer dừng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp

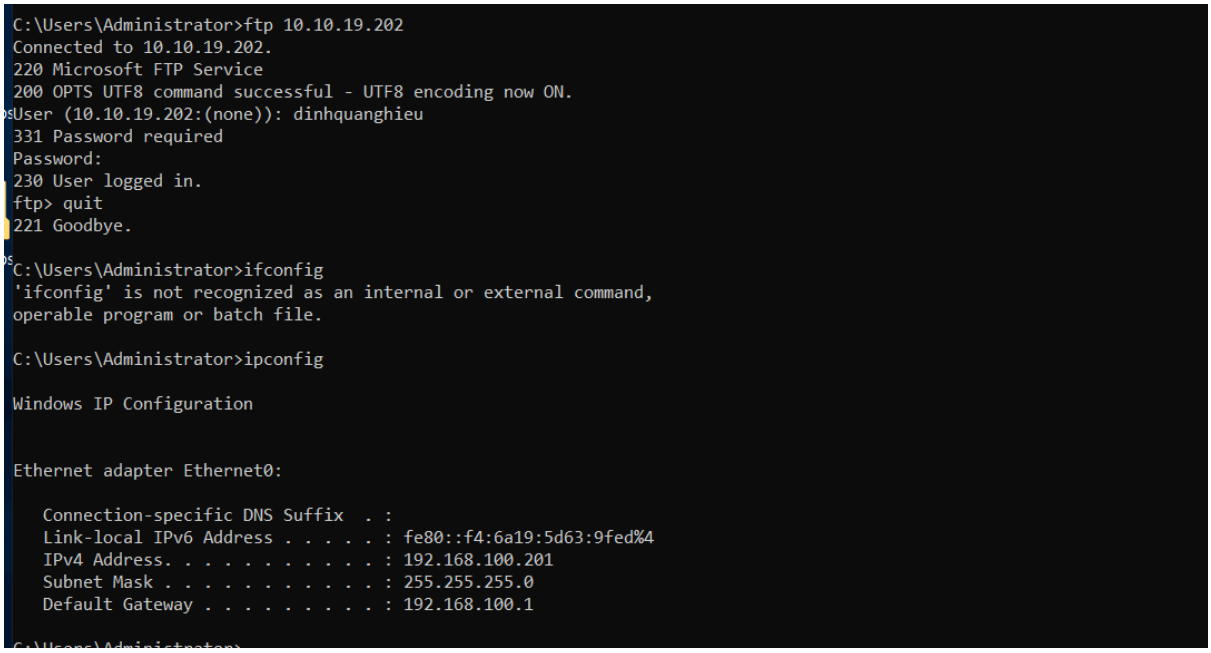


- Trên máy Windows attack, trong Capture Interfaces chọn Start ở dòng eth1 để bắt gói tin trên dải mạng 192.168.100.0

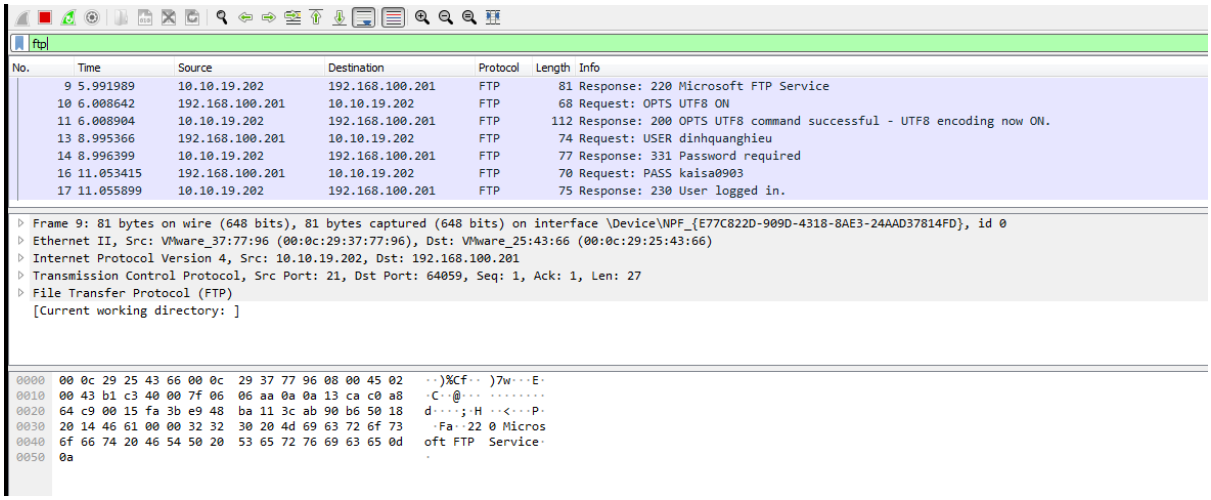


- Trên máy Window Server 2003 victim, kết nối với ftp server (root@bt:~#ftp 10.10.19.202)





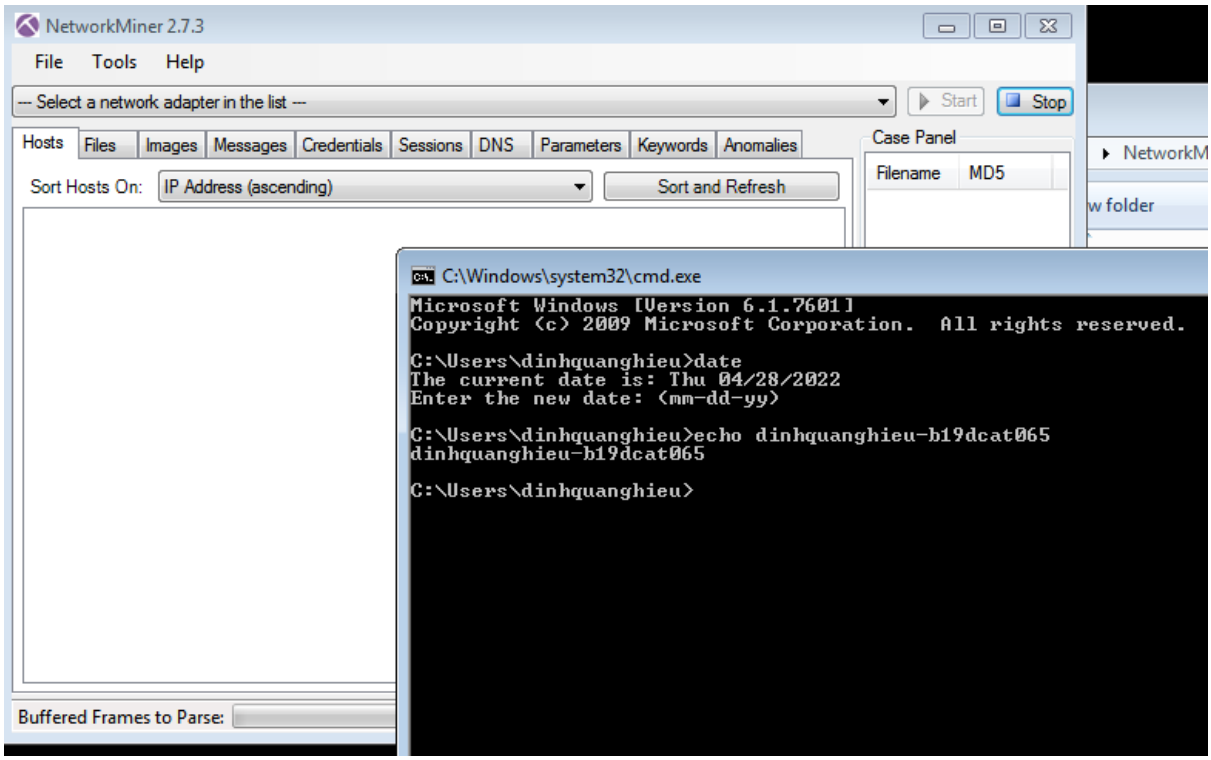
- Trên Window 7 dừng quá trình bắt gói tin và lọc theo giao thức ftp



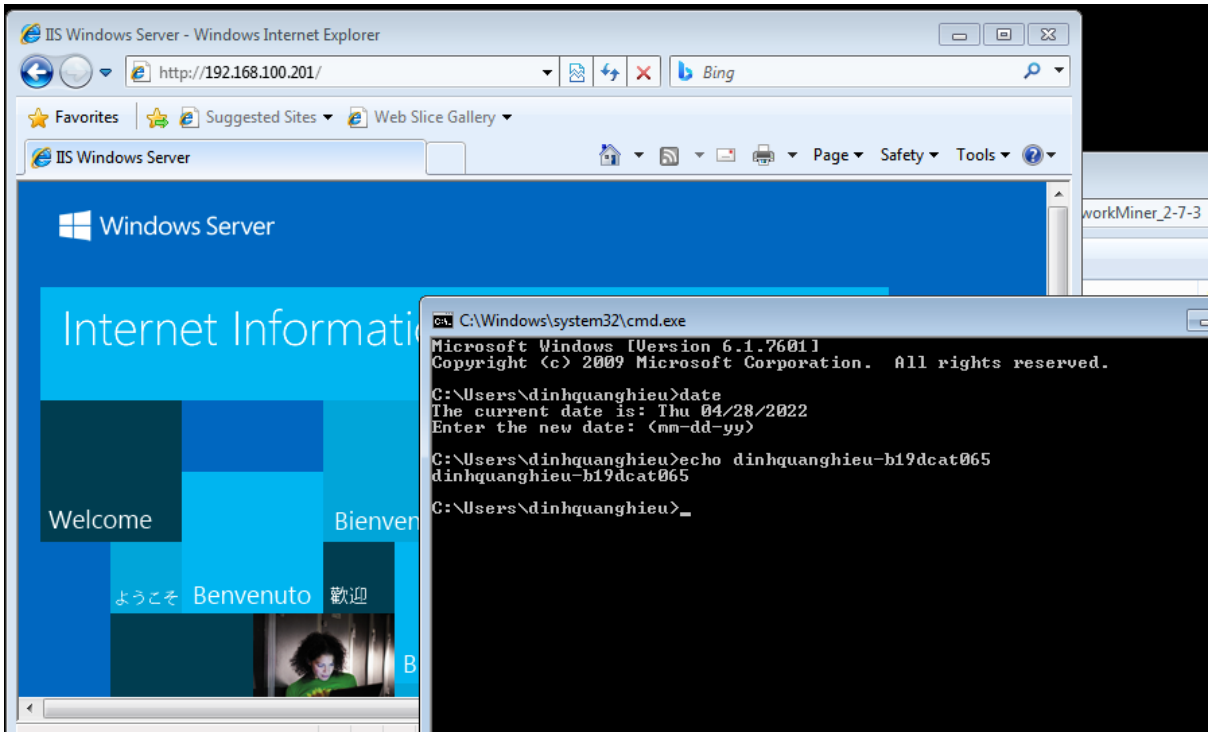
- Sử dụng Network Miner để bắt và phân tích các gói tin

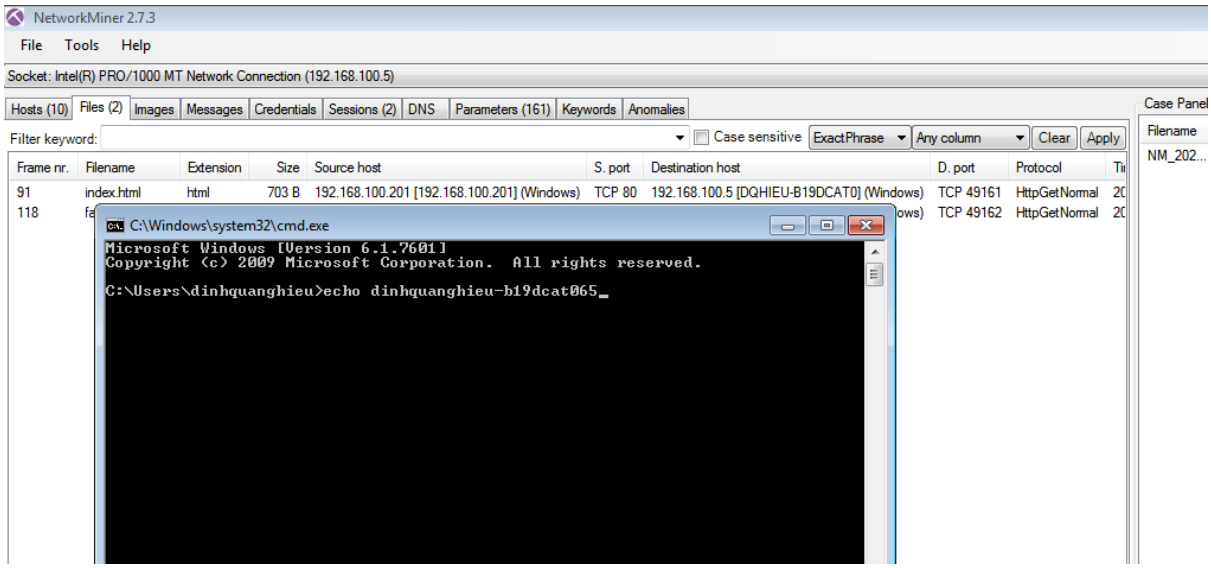
a) Các bước thực hiện

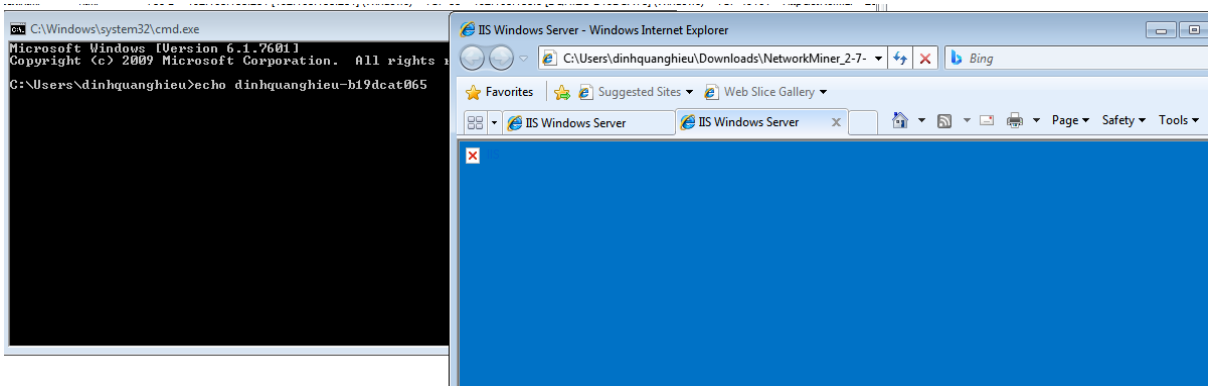
o Trên máy Windows 7 Internal Attack khởi động và chọn Socket: Intel® PRO/1000MT Network Connection(192.168.100.5) và bắt đầu bắt gói tin.



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


IIS Windows Server - Windows Internet Explorer
http://192.168.100.201/
Bing
Favorites
Suggested Sites
Web Slice Gallery
IIS Windows Server
Page
Safety
Tools
Windows Server
Internet Informati
Welcome
Bienven
ようこそ
Benvenuto
歡迎
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\dinhquanghieu>date
The current date is: Thu 04/28/2022
Enter the new date: (mm-dd-yy)
C:\Users\dinhquanghieu>echo dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065
C:\Users\dinhquanghieu>


NetworkMiner 2.7.3
File
Tools
Help
Socket: Intel(R) PRO/1000 MT Network Connection (192.168.100.5)
Hosts (10)
Files (2)
Images
Messages
Credentials
Sessions (2)
DNS
Parameters (161)
Keywords
Anomalies
Case Panel
Filter keyword:
Case sensitive
ExactPhrase
Any column
Clear
Apply
Frame nr.
Filename
Extension
Size
Source host
S. port
Destination host
D. port
Protocol
91
index.html
html
703 B
192.168.100.201 [192.168.100.201] (Windows)
TCP 80
192.168.100.5 [DQHIEU-B19DCAT0] (Windows)
TCP 49161
HttpGetNormal
118
TCP 49162
HttpGetNormal
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\dinhquanghieu>echo dinhquanghieu-b19dcat065


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights
C:\Users\dinhquanghieu>echo dinhquanghieu-b19dcat065
IIS Windows Server - Windows Internet Explorer
C:\Users\dinhquanghieu\Downloads\NetworkMiner_2-7-
Bing
Favorites
Suggested Sites
Web Slice Gallery
IIS Windows Server
IIS Windows Server
Page
Safety
Tools