Báo cáo bài thực hành số 8

Môn học

Thực tập cơ sở

Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

Mã SV: B19DCAT141

I. Lý thuyết:

- **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,…
- **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
- **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.

II. Thực hành:

- 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(thời gian chờ dữ liệu trong khoảng 5 phút)

```
┌──(kali㉿b19dcat141-phuong-kali)-[~]
└─$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.19.4  netmask 255.0.0.0  broadcast 10.255.255.255
        ether 00:0c:29:c1:39:6a  txqueuelen 1000  (Ethernet)
        RX packets 17  bytes 1588 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 38  bytes 5461 (5.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.4  netmask 255.255.255.0  broadcast 192.168.100.255
        ether 00:0c:29:c1:39:74  txqueuelen 1000  (Ethernet)
        RX packets 16  bytes 1528 (1.4 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

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
```

```
┌──(kali㉿b19dcat141-phuong-kali)-[~]
└─$ sudo timeout 120 tcpdump -i eth1 -v -w Desktop/data1.pcaps
```

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

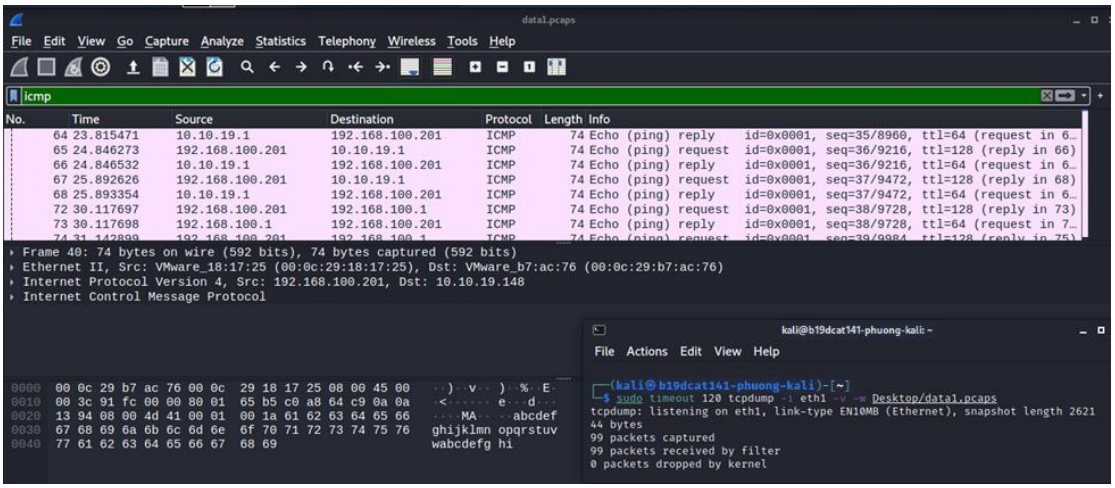
```
Administrator: Command Prompt - ftp 192.168.100.147

C:\>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=2ms TTL=63
Reply from 10.10.19.148: bytes=32 time=2ms 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 = 2ms, Average = 1ms

C:\>ping 192.168.100.147

Pinging 192.168.100.147 with 32 bytes of data:
Reply from 192.168.100.147: bytes=32 time=1024ms 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 = 1024ms, Average = 256ms

C:\>
```

```
Command Prompt
(c) 2018 Microsoft Corporation. All rights reserve

C:\Users\phuong-b19dcat141>echo "Nguyen Minh Phu
"Nguyen Minh Phuong-B19DCAT141"

C:\Users\phuong-b19dcat141>
```

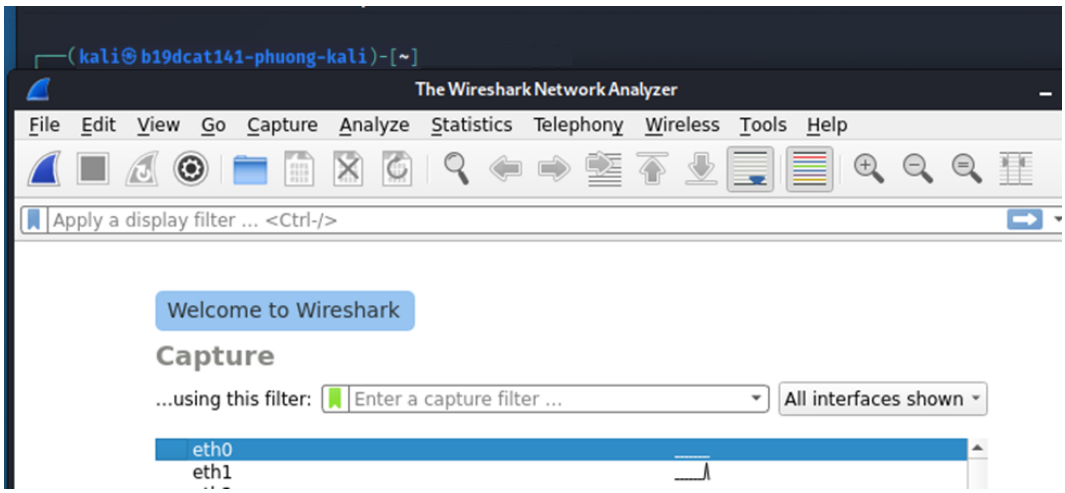
- Trên máy Linux Sniffer, tiến hành bắt gói tin bằng tcpdump, và lưu dữ liệu vào file pcap.

```
┌──(kali㉿b19dcat141-phuong-kali)-[~]
└─$ sudo timeout 120 tcpdump -i eth1 -v -w Desktop/data1.pcaps
tcpdump: listening on eth1, link-type EN10MB (Ethernet), snapshot length 2621
44 bytes
99 packets captured
99 packets received by filter
0 packets dropped by kernel
```

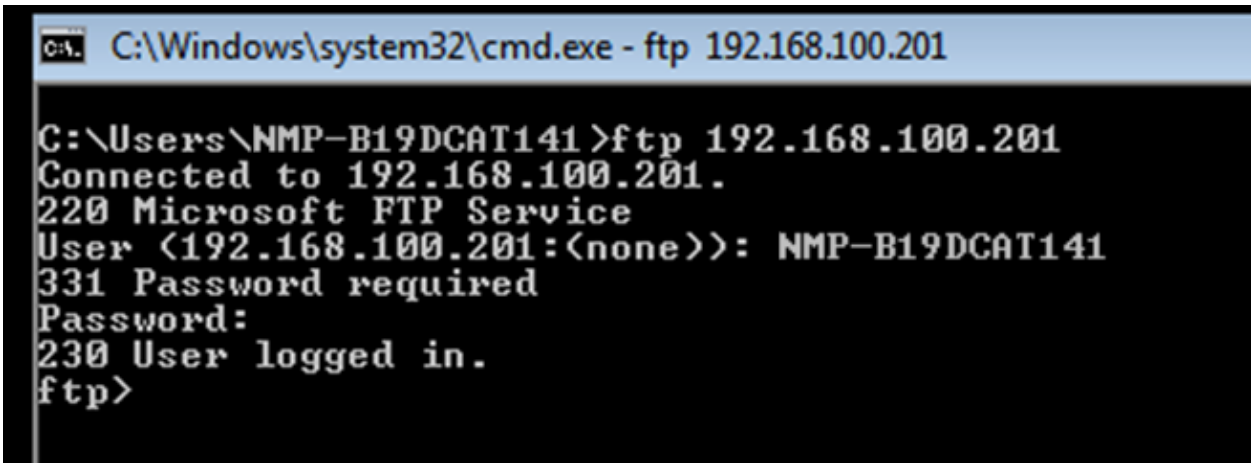
- Kết quả cần đạt được
  + Thu được kết quả bắt gói tin và các file pcap thông qua tcpdump



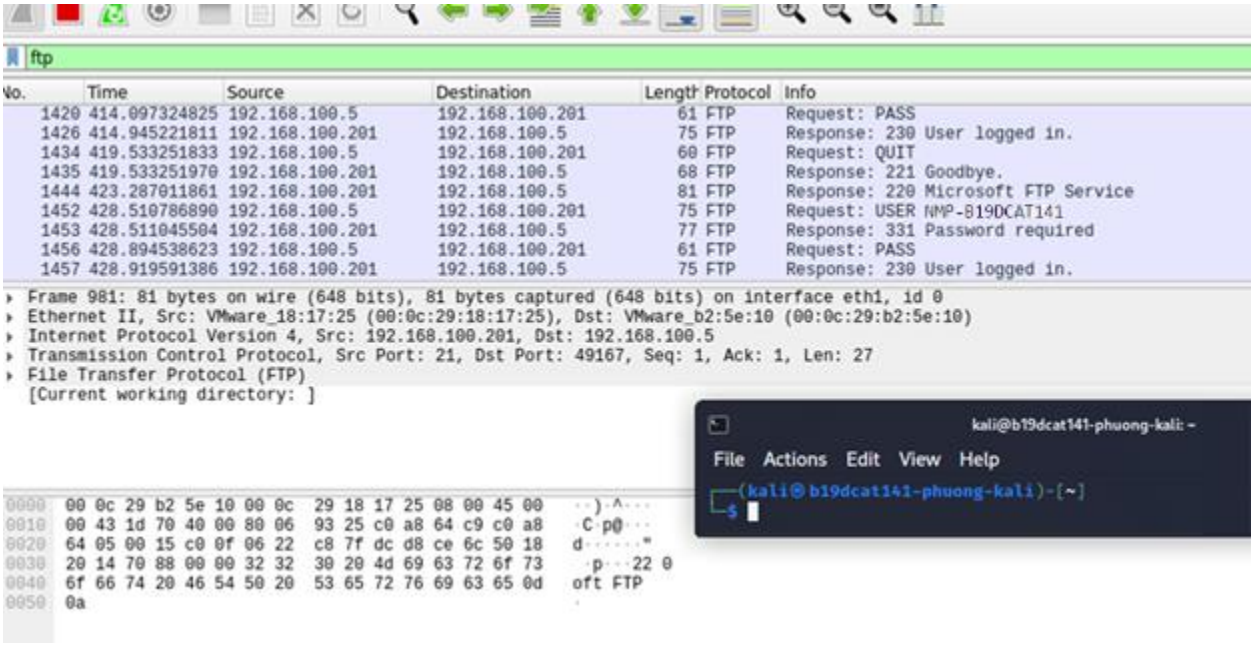
- Sử dụng Wireshark để bắt và phân tích các gói tin
  + Trên máy Linux Sniffer, bật các interfaces eth0, eth1 và khởi động Wireshark. Trong Capture Interfaces chọn Start ở dòng eth1 để bắt gói tin trên dải mạng 192.168.100.0



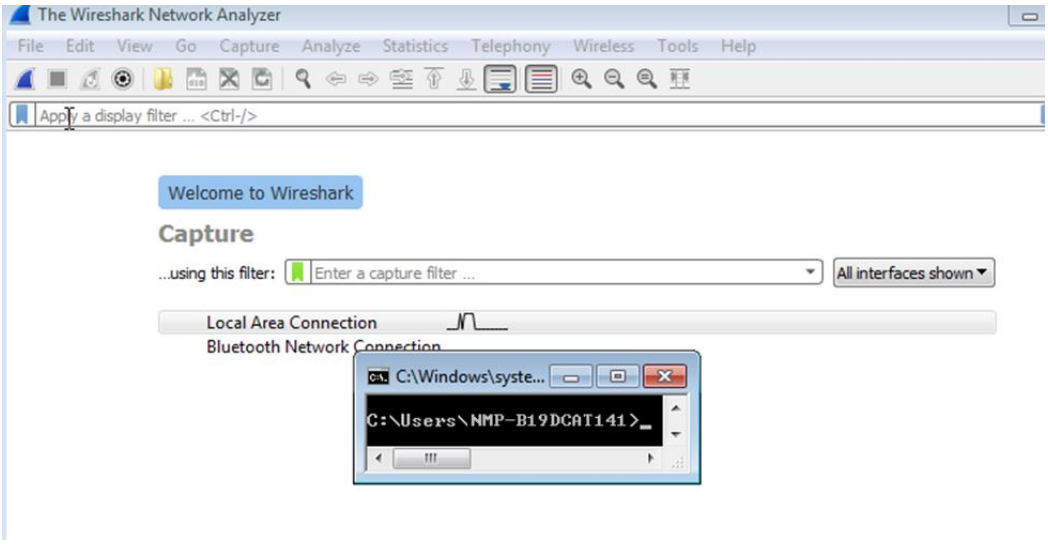
+ Trên máy Windows 7 Attack kết nối tới ftp server (C:\ftp 192.168.100.201) trên máy Window Server Internal Victim



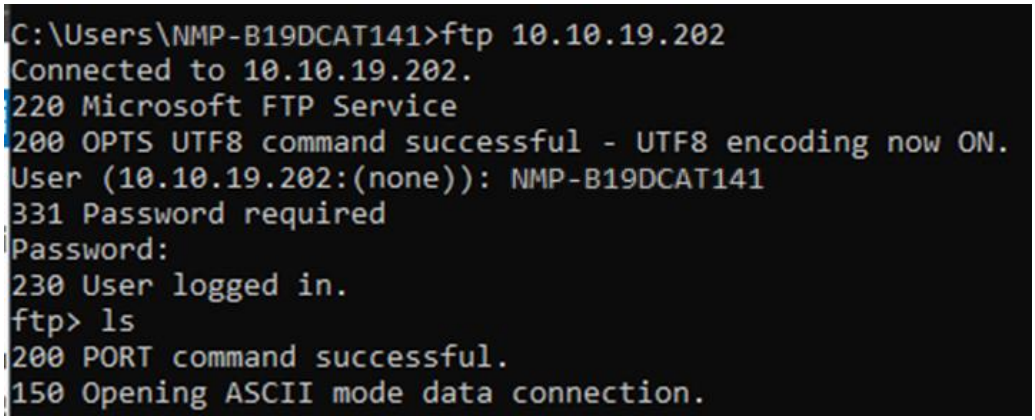
+ Trên Linux Sniffer dừng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp



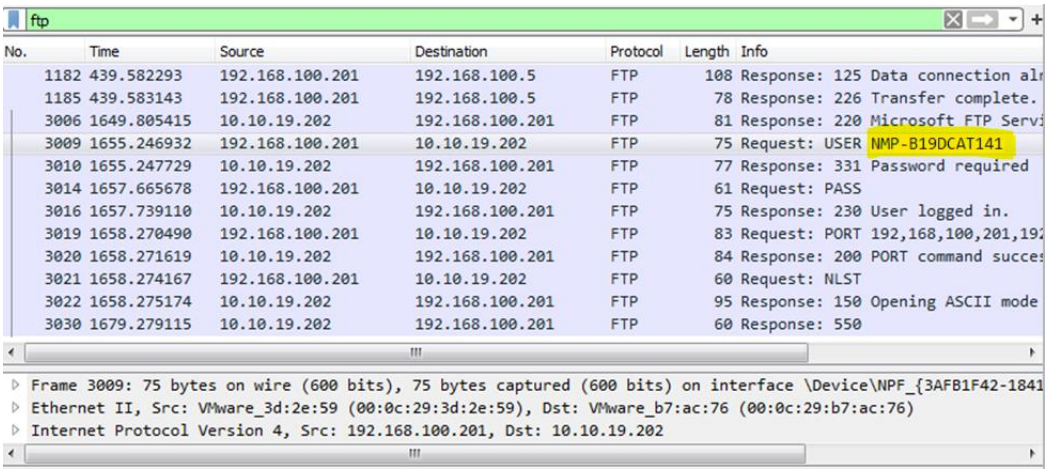
+ Trên máy Windows attack, trong Capture Interfaces chọn Start ở dòng eth1 để bắt gói tin trên dải mạng 192.168.100.0



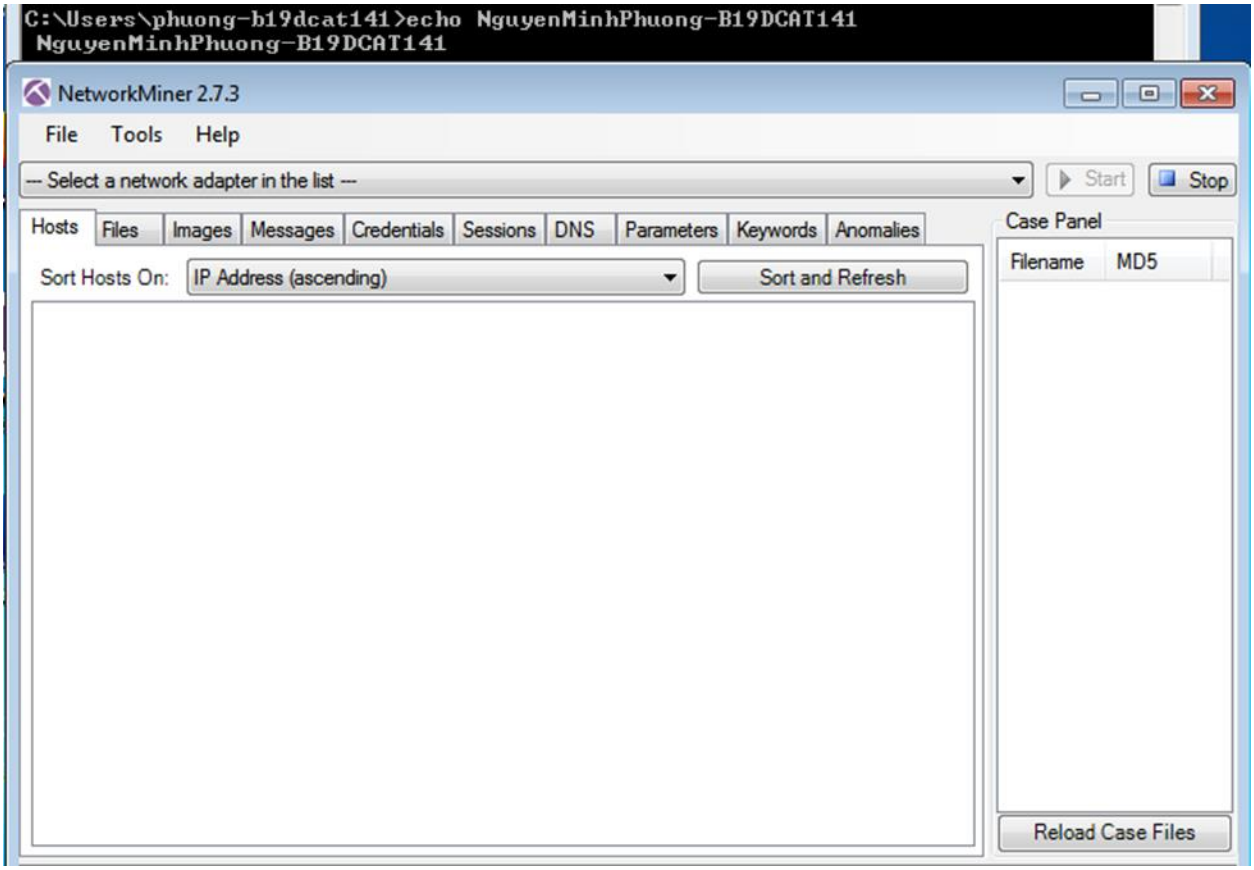
+ Trên máy Window Server 2003 victim, kết nối với ftp server(root@bt:~#ftp 10.10.19.202)



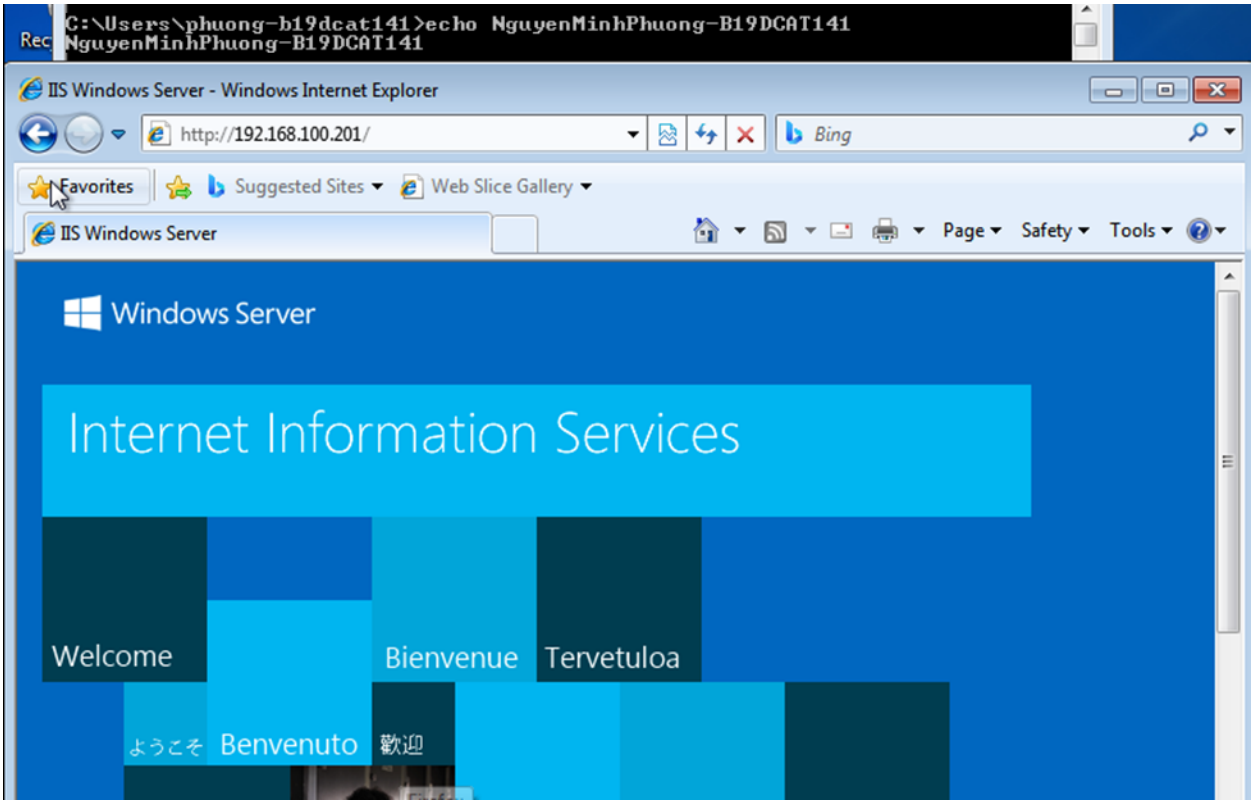
+ Trên Window 7 dừng quá trình bắt gói tin và lọc theo giao thức ftp



- Sử dụng Networkminer để bắt và phân tích các gói tin
    + Trên máy Windows 7 Internal Attack khởi động Networkminer và chọn Socket: Intel® PRO/1000 MT 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.