

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 0x10<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 reserved.

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

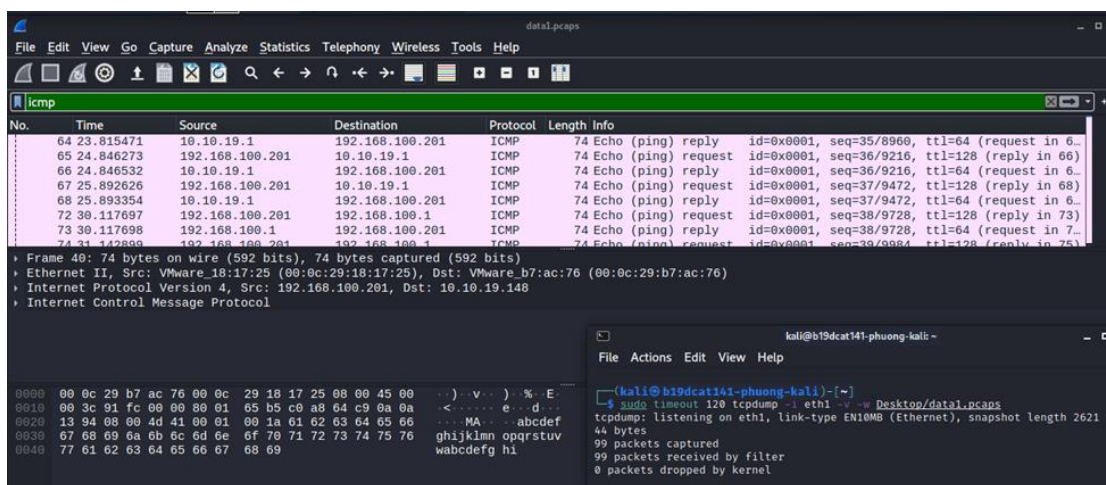
C:\Users\phuong-b19dcat141>

```

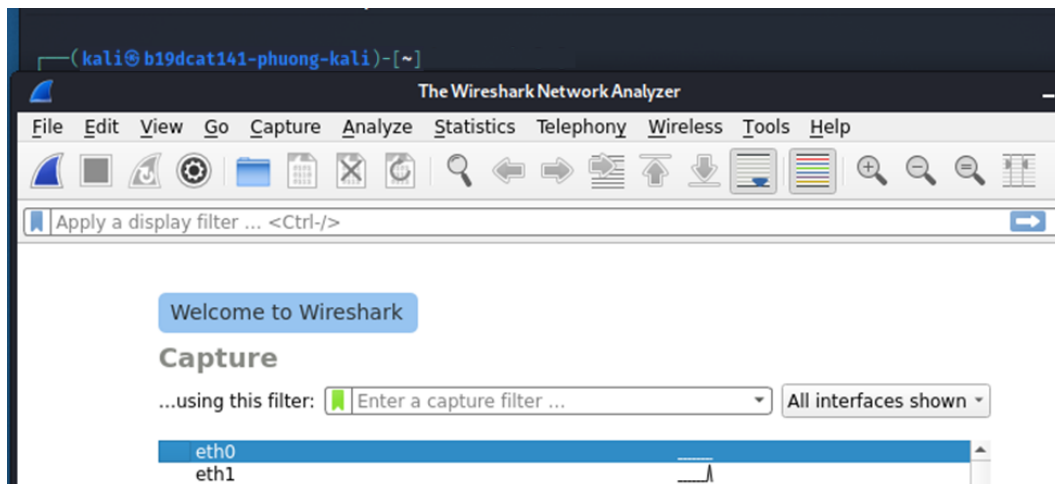
- Trên máy Linux Sniffer, tiến hành bắt gói tin bằng tcpdump, và lưu dữ liệu vào file pcap.

```
(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

```
C:\Windows\system32\cmd.exe - ftp 192.168.100.201

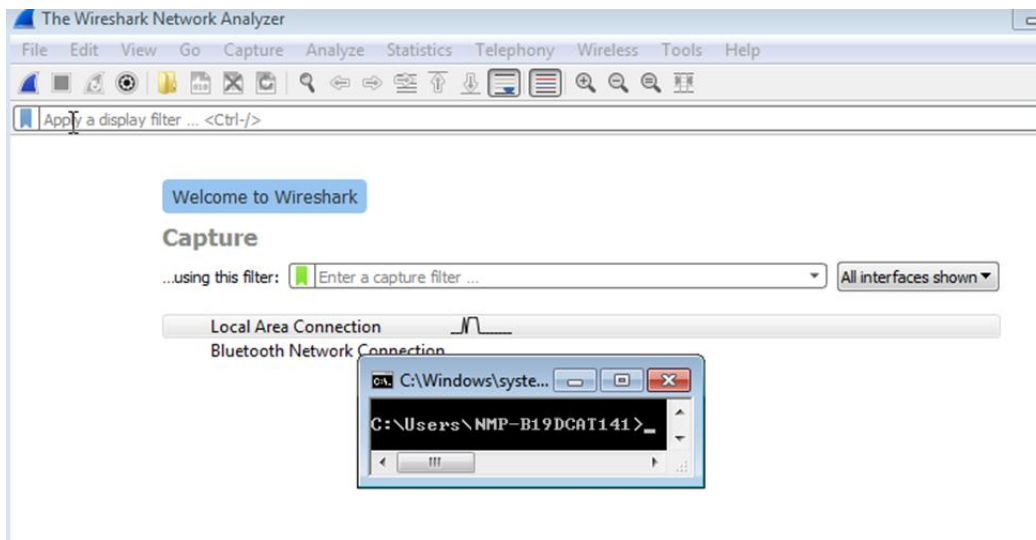
C:\Users\NMP-B19DCAT141>ftp 192.168.100.201
Connected to 192.168.100.201.
220 Microsoft FTP Service
User (192.168.100.201:(none)): NMP-B19DCAT141
331 Password required
Password:
230 User logged in.
ftp>
```

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

The screenshot displays the Wireshark network traffic analysis tool. The main pane shows a list of captured packets, with the selected packet (No. 1457) being an FTP 'User logged in' response. The details pane on the right shows the hierarchical structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and File Transfer Protocol (FTP). In the foreground, a terminal window shows the Kali Linux command prompt, indicating the user is at the kali@b19dcat141-phuong-kali machine.

No.	Time	Source	Destination	Length	Protocol	Info
1420	414.097324825	192.168.100.5	192.168.100.201	61	FTP	Request: PASS
1426	414.945221811	192.168.100.201	192.168.100.5	75	FTP	Response: 230 User logged in.
1434	419.533251833	192.168.100.5	192.168.100.201	60	FTP	Request: QUIT
1435	419.533251970	192.168.100.201	192.168.100.5	68	FTP	Response: 221 Goodbye.
1444	423.287911861	192.168.100.201	192.168.100.5	81	FTP	Response: 220 Microsoft FTP Service
1452	428.510786890	192.168.100.5	192.168.100.201	75	FTP	Request: USER NMP-B19DCAT141
1453	428.511045504	192.168.100.201	192.168.100.5	77	FTP	Response: 331 Password required
1456	428.894538623	192.168.100.5	192.168.100.201	61	FTP	Request: PASS
1457	428.919591386	192.168.100.201	192.168.100.5	75	FTP	Response: 230 User logged in.

- + 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)

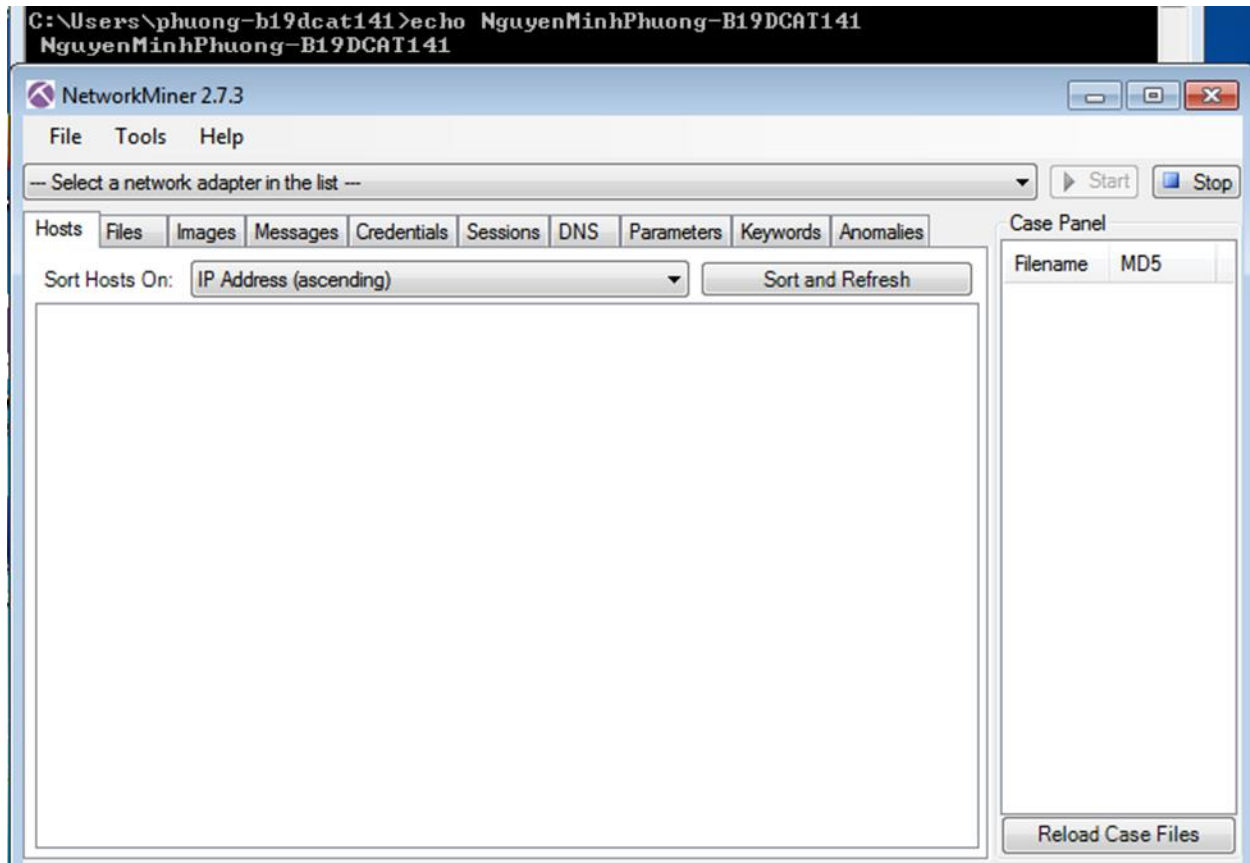
```
C:\Users\NMP-B19DCAT141>ftp 10.10.19.202
Connected to 10.10.19.202.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (10.10.19.202:(none)): NMP-B19DCAT141
331 Password required
Password:
230 User logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
```

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

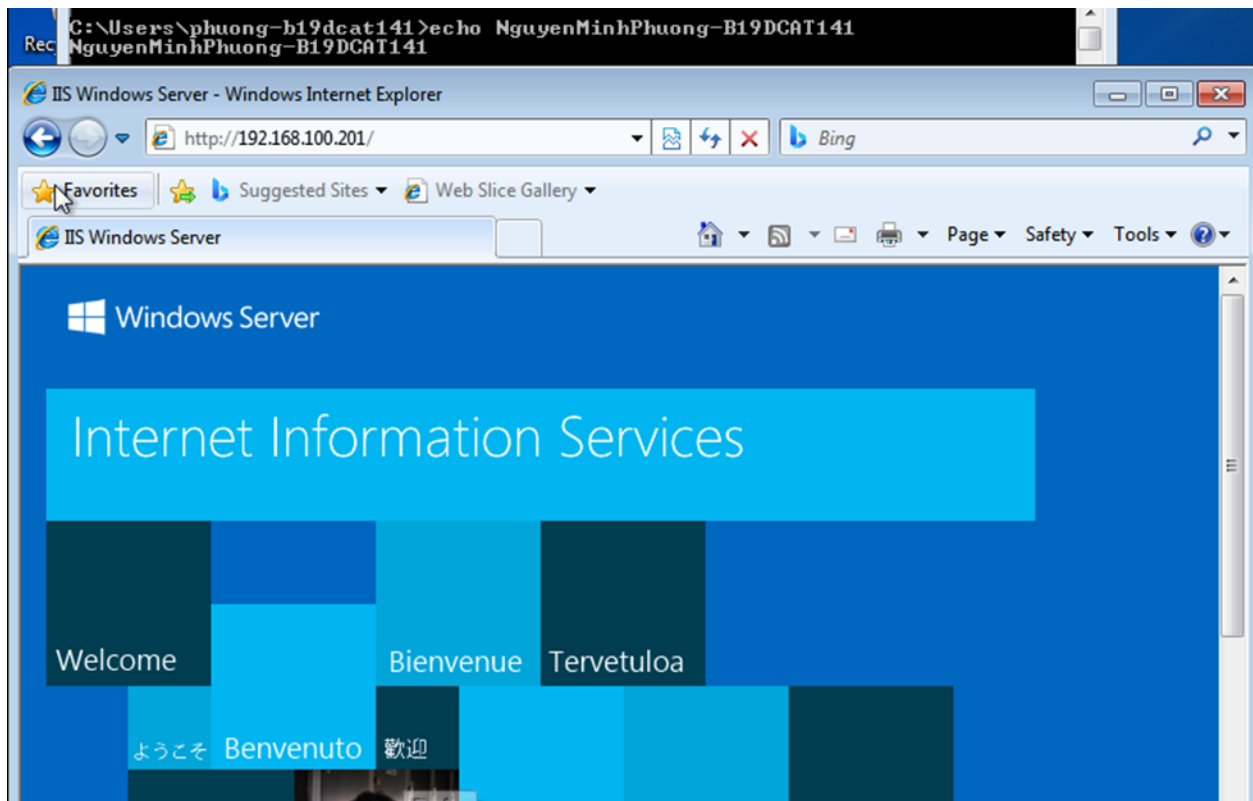
No.	Time	Source	Destination	Protocol	Length	Info
1182	439.582293	192.168.100.201	192.168.100.5	FTP	108	Response: 125 Data connection already open; transfer starting.
1185	439.583143	192.168.100.201	192.168.100.5	FTP	78	Response: 226 Transfer complete.
3006	1649.805415	10.10.19.202	192.168.100.201	FTP	81	Response: 220 Microsoft FTP Service.
3009	1655.246932	192.168.100.201	10.10.19.202	FTP	75	Request: USER NMP-B19DCAT141
3010	1655.247729	10.10.19.202	192.168.100.201	FTP	77	Response: 331 Password required.
3014	1657.665678	192.168.100.201	10.10.19.202	FTP	61	Request: PASS
3016	1657.739110	10.10.19.202	192.168.100.201	FTP	75	Response: 230 User logged in.
3019	1658.270490	192.168.100.201	10.10.19.202	FTP	83	Request: PORT 192,168,100,201,192,168,100,201
3020	1658.271619	10.10.19.202	192.168.100.201	FTP	84	Response: 200 PORT command successful.
3021	1658.274167	192.168.100.201	10.10.19.202	FTP	60	Request: NLST
3022	1658.275174	10.10.19.202	192.168.100.201	FTP	95	Response: 150 Opening ASCII mode data connection.
3030	1679.279115	10.10.19.202	192.168.100.201	FTP	60	Response: 550

Frame 3009: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{3AFB1F42-1841-408D-8000-000000000000} Ethernet II, Src: VMware_3d:2e:59 (00:0c:29:3d:2e:59), Dst: VMware_b7:ac:76 (00:0c:29:b7:ac:76)
Internet Protocol Version 4, Src: 192.168.100.201, Dst: 10.10.19.202

- 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 dùng quá trình bắt gói tin.



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

