

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



Môn: Thực tập cơ sở

BÁO CÁO THỰC TẬP CƠ SỞ
Bài 11: Bắt và phân tích gói tin trong mạng

Họ và tên giảng viên:	<i>PGS.TS.Đỗ Xuân Chợt</i>
Họ và tên:	<i>Phạm Thanh Tùng</i>
Mã sinh viên:	<i>B20DCAT171</i>
Lớp:	<i>D20CQAT03-B</i>
Số điện thoại:	<i>0856915668</i>

Hà Nội 2023

1. Mục đích:

- Bài thực hành này giúp sinh viên nắm được công cụ và cách thức bắt dữ liệu mạng, bao gồm:
 - 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. Nội dung thực hành:

2.1. Tìm hiểu lý thuyết:

- Sniffer hay packet sniffer là một chương trình phần mềm nghe trộm gói tin (còn gọi là chương trình phân tích mạng, phân tích giao thức hay nghe trộm Ethernet), có khả năng chặn bắt và ghi lại lưu lượng dữ liệu qua một mạng viễn thông số hoặc một phần của một mạng. Khi các dòng dữ liệu di chuyển qua lại trong một mạng, chương trình sẽ chặn bắt các gói tin rồi giải mã và phân tích nội dung của nó theo đặc tả RFC hoặc các đặc tả thích hợp khác.
- Sniffer hoạt động theo phương thức chặn Network Traffic, người dùng có thể nhìn thấy thông tin thông qua mạng dây hoặc mạng không dây mà chính phần mềm này đã truy cập trên máy chủ.
- Dựa theo cách hoạt động này, các Hacker có thể sử dụng Sniffer để nghe trộm trên những thông tin, dữ liệu chưa được mã hóa và xem được toàn bộ thông tin được trao đổi giữa hai bên. Ngoài ra những thông tin mật như mật khẩu, xác nhận mật khẩu cũng bị các Hacker thu thập.
- Một số 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#>

2.2. Các bước thực hiện

2.2.1. Sử dụng tcpdump

- Đăng nhập Linux Sniffer và xem tất cả các interfaces trong hệ thống (root@bt:~#**ifconfig -a**) sau đó khởi động tcpdump. Bắt gói tin trên dải mạng 192.168.100.0/24 và gửi vào một file

```
tungpt171@tungpt171: ~/Desktop
tungpt171@tungpt171:~/Desktop$ ifconfig -a
ens33: flags=4098<BROADCAST,MULTICAST> mtu 1500
    ether 00:0c:29:39:ad:34 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    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

ens37: flags=4098<BROADCAST,MULTICAST> mtu 1500
    ether 00:0c:29:39:ad:3e txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    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)
    RX packets 179 bytes 13981 (13.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 179 bytes 13981 (13.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tungpt171@tungpt171:~$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
tungpt171@tungpt171:~$ date
Thứ sáu, 10 Tháng 3 năm 2023 17:36:37 +07
tungpt171@tungpt171:~$
```

- Kích hoạt các interfaces(eth0, eth1) hoạt động ở chế độ hỗn hợp,

```
tungpt171@tungpt171: ~/Desktop
tungpt171@tungpt171:~/Desktop$ sudo ifconfig ens33 -promisc
[sudo] password for tungpt171:
tungpt171@tungpt171:~/Desktop$ sudo ifconfig ens37 -promisc
tungpt171@tungpt171:~/Desktop$

tungpt171@tungpt171:~$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
tungpt171@tungpt171:~$ date
Thứ sáu, 10 Tháng 3 năm 2023 17:36:37 +07
tungpt171@tungpt171:~$
```

- Kích hoạt các interfaces

```
tungpt171@tungpt171: ~/Desktop
tungpt171@tungpt171:~/Desktop$ sudo ifconfig ens33 up
tungpt171@tungpt171:~/Desktop$ sudo ifconfig ens37 up
tungpt171@tungpt171:~/Desktop$ ifconfig -a
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::20c:29ff:fe39:ad34  prefixlen 64  scopeid 0x20<
link>
        ether 00:0c:29:39:ad:34  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 2645 (2.6 KB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::20c:29ff:fe39:ad3e  prefixlen 64  scopeid 0x20<
link>
        ether 00:0c:29:39:ad:3e  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19  bytes 2468 (2.4 KB)
        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>

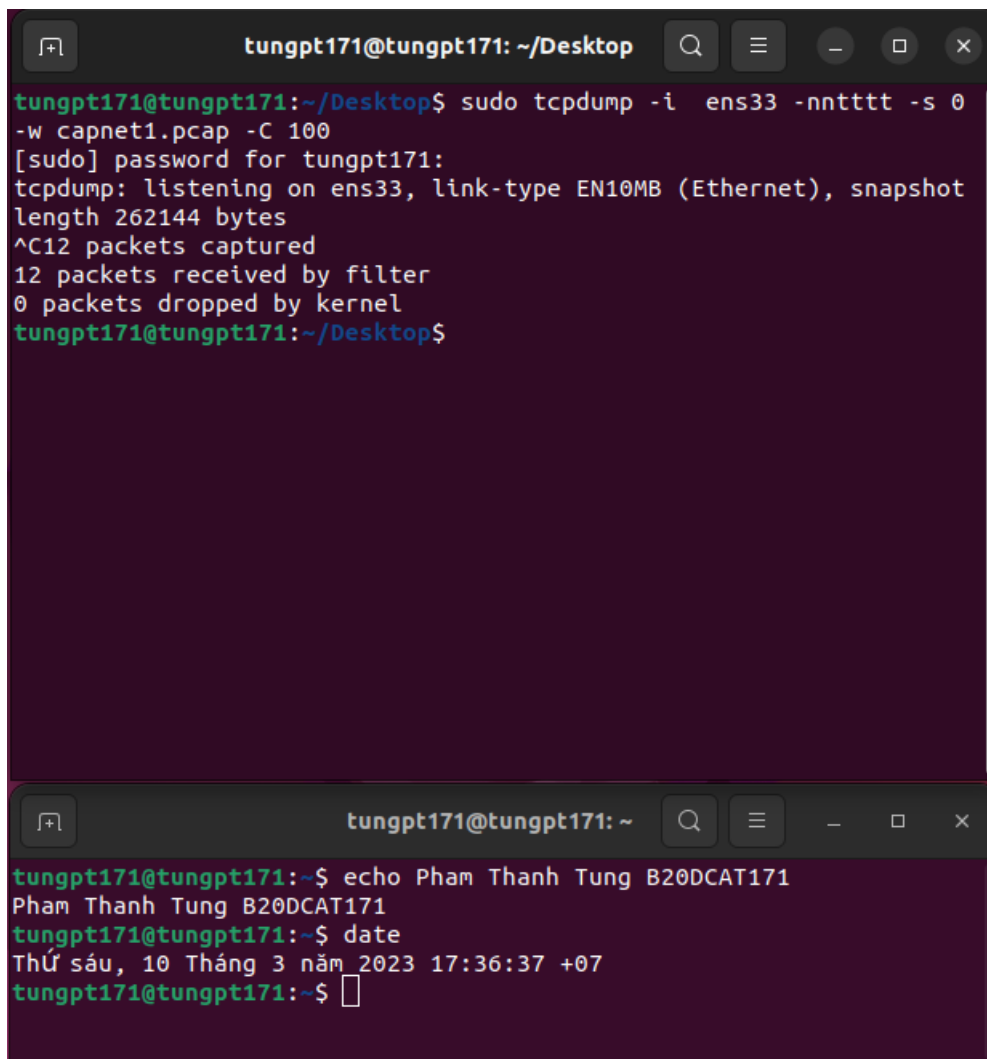
tungpt171@tungpt171:~$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
tungpt171@tungpt171:~$ date
Thứ sáu, 10 Tháng 3 năm 2023 17:36:37 +07
tungpt171@tungpt171:~$
```

- Bắt gói tin trên dải mạng 192.168.100.0/24

```
tungpt171@tungpt171: ~/Desktop
tungpt171@tungpt171:~/Desktop$ sudo tcpdump -i ens33
[sudo] password for tungpt171:
tcpdump: verbose output suppressed, use -v[v]... for full protocol
decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 26
2144 bytes
18:12:15.821911 IP 192.168.100.147 > 192.168.100.1: ICMP echo reque
st, id 2, seq 1, length 64
18:12:15.821911 IP 192.168.100.1 > 192.168.100.147: ICMP echo reply
, id 2, seq 1, length 64
18:12:16.822824 IP 192.168.100.147 > 192.168.100.1: ICMP echo reque
st, id 2, seq 2, length 64
18:12:16.822982 IP 192.168.100.1 > 192.168.100.147: ICMP echo reply
, id 2, seq 2, length 64
18:12:17.830190 IP 192.168.100.147 > 192.168.100.1: ICMP echo reque
st, id 2, seq 3, length 64
18:12:17.830230 IP 192.168.100.1 > 192.168.100.147: ICMP echo reply
, id 2, seq 3, length 64
18:12:18.854016 IP 192.168.100.147 > 192.168.100.1: ICMP echo reque
st, id 2, seq 4, length 64
18:12:18.854017 IP 192.168.100.1 > 192.168.100.147: ICMP echo reply
, id 2, seq 4, length 64
18:12:19.877749 IP 192.168.100.147 > 192.168.100.1: ICMP echo reque
st, id 2, seq 5, length 64

tungpt171@tungpt171: ~
tungpt171@tungpt171:~$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
tungpt171@tungpt171:~$ date
Thứ sáu, 10 Tháng 3 năm 2023 17:36:37 +07
tungpt171@tungpt171:~$
```

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



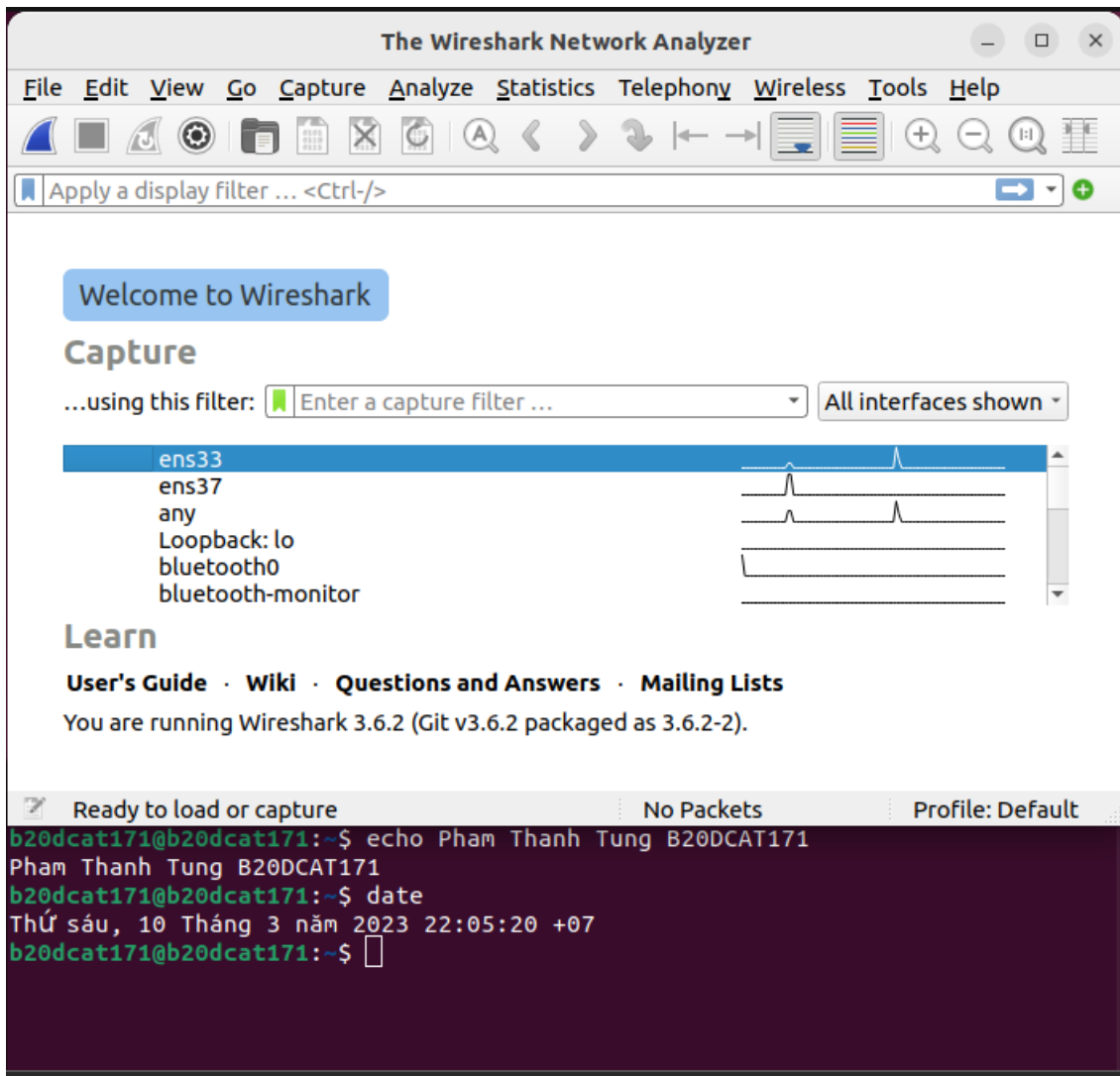
The image displays two terminal windows from a Linux system. The top window shows the execution of the `sudo tcpdump` command to capture traffic on the `ens33` interface. The output indicates that 12 packets were received by the filter and 0 were dropped by the kernel. The bottom window shows the execution of `echo` and `date` commands, displaying the system's name and the current date and time.

```
tungpt171@tungpt171: ~/Desktop
tungpt171@tungpt171:~/Desktop$ sudo tcpdump -i ens33 -nntttt -s 0
-w capnet1.pcap -C 100
[sudo] password for tungpt171:
tcpdump: listening on ens33, link-type EN10MB (Ethernet), snapshot
length 262144 bytes
^C12 packets captured
12 packets received by filter
0 packets dropped by kernel
tungpt171@tungpt171:~/Desktop$

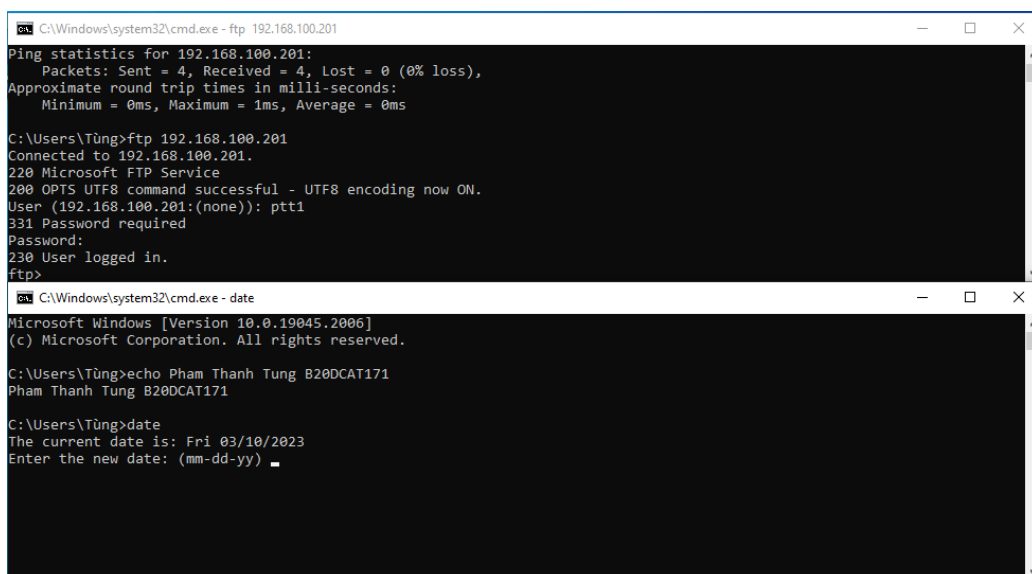
tungpt171@tungpt171: ~
tungpt171@tungpt171:~$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
tungpt171@tungpt171:~$ date
Thứ sáu, 10 Tháng 3 năm 2023 17:36:37 +07
tungpt171@tungpt171:~$
```

2.2.2. Sử dụng Wireshark để bắt và phân tích các gói tin

- Mở wireshake và xem các interface có sẵn



- Sử dụng interface nhận lưu lượng từ 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



- Bắt gói tin từ mạng 192.168.100.0

The image shows two windows. The top window is Wireshark, titled 'Capturing from ens33'. It displays a list of captured packets. The bottom window is a Linux terminal with the prompt 'b20dcat171@b20dcat171: ~'.

Wireshark Packet List:

No.	Time	Source	Destination	Protocol	Length
4	5.242887315	VMware_e2:ab:57	VMware_aa:1e:0f	ARP	
5	8.396920318	192.168.100.5	192.168.100.201	ICMP	
6	8.397199772	192.168.100.201	192.168.100.5	ICMP	
7	9.406113790	192.168.100.5	192.168.100.201	ICMP	

Wireshark Packet Details (Frame 1):

- Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface
- Ethernet II, Src: VMware_aa:1e:0f (00:0c:29:aa:1e:0f), Dst: VMware_e2:ab:57
- Internet Protocol Version 4, Src: 192.168.100.134, Dst: 185.125.190.56
- User Datagram Protocol, Src Port: 40540, Dst Port: 123
- Network Time Protocol (NTP Version 4, client)

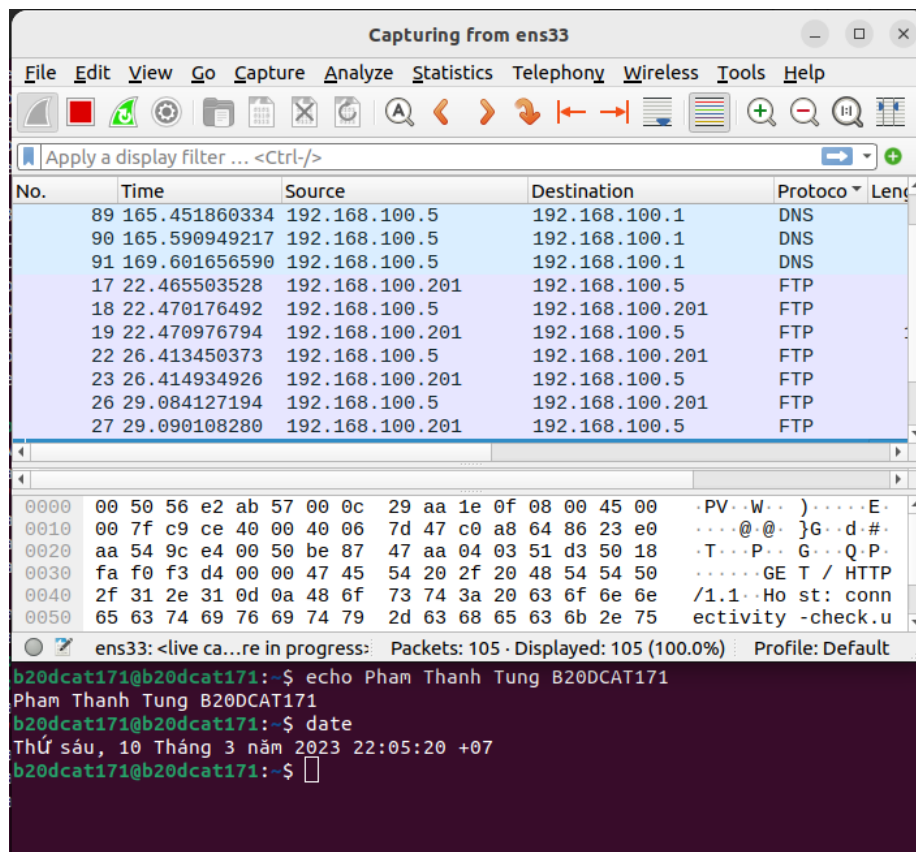
Wireshark Packet Bytes:

Offset	Bytes	ASCII
0000	00 50 56 e2 ab 57 00 0c 29 aa 1e 0f 08 00 45 10	·PV··W··)·...·E·
0010	00 4c 02 3a 40 00 40 11 9b 72 c0 a8 64 86 b9 7d	·L·:@·@· ·r·d·}
0020	be 38 9e 5c 00 7b 00 38 9d 2e 23 00 00 00 00 00	·8·\·{·8·.·#·...·
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Linux Terminal Output:

```
b20dcat171@b20dcat171:~$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
b20dcat171@b20dcat171:~$ date
Thứ sáu, 10 Tháng 3 năm 2023 22:05:20 +07
b20dcat171@b20dcat171:~$
```

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



2.2.3. Sử dụng Network Miner

- Trên máy Windows Internal Attack khởi động Network Miner và chọn Socket: Network Connection(192.168.100.5) và bắt đầu bắt gói tin

