Міністерство освіти і науки України

Львівський національний університет імені Івана Франка

Факультет електроніки та комп’ютерних технологій

Звіт

Про виконання лабораторної роботи №8

З курсу «Комп'ютерні інформаційні мережі»

« Стек протоколів »

Виконав:

Студент групи ФеС-21

Шавало Андрій

Львів-2025

Мета: Отримати практичний досвід роботи з протоколами TCP/IP, UPD, ICMP.

ХІД РОБОТИ

1. За потреби встановити утиліту tcpdump

```
andriy@sos:~$ tcpdump -h
tcpdump version 4.99.4
libpcap version 1.10.4 (with TPACKET_V3)
OpenSSL 3.0.13 30 Jan 2024
Usage: tcpdump [-AbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ] [--count]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ --immediate-mode ] [ -j tstamptype ]
                [ -M secret ] [ --number ] [ --print ] [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ -T type ] [ --version ]
                [ -V file ] [ -w file ] [ -W filecount ] [ -y datalinktype ]
                [ --time-stamp-precision precision ] [ --micro ] [ --nano ]
                [ -z postrotate-command ] [ -Z user ] [ expression ]
```

2. За допомогою tcpdump

a. продемонструвати перехоплення авторизаційних даних (логін і пароль) при авторизації в Wordpress

```
andriy@sos:~$ sudo tcpdump -i enp0s3 -A port 80
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

```
log=Andriy&pwd=J2e38mTSZCTL%26TX0c3&wp-submit=%D0%92%D0%BE
%D0%B9%D1%82%D0%B8&redirect_to=http%3A%2F%2Flocalhost%3A80
00%2Fwp-admin%2F&testcookie=1
```

b. продемонструвати трафік до DNS сервера

```
andriy@sos:~$ sudo tcpdump -i enp0s3 port 53 -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:19:08.213917 IP 10.0.2.15.33239 > 10.0.2.3.53: 46317+ [1au] A? incoming.telem
etry.mozilla.org. (59)
15:19:08.214379 IP 10.0.2.15.60036 > 10.0.2.3.53: 16754+ [1au] AAAA? incoming.te
lemetry.mozilla.org. (59)
15:19:08.230269 IP 10.0.2.3.53 > 10.0.2.15.33239: 46317 2/0/1 CNAME telemetry-in
coming.r53-2.services.mozilla.com., A 34.120.208.123 (134)
15:19:08.230269 IP 10.0.2.3.53 > 10.0.2.15.60036: 16754 1/1/1 CNAME telemetry-in
coming.r53-2.services.mozilla.com. (197)
15:19:08.231403 IP 10.0.2.15.57353 > 10.0.2.3.53: 39375+ [1au] AAAA? telemetry-i
ncoming.r53-2.services.mozilla.com. (74)
15:19:08.241204 IP 10.0.2.3.53 > 10.0.2.15.57353: 39375 0/1/1 (156)
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
```

c. продемонструвати перехоплення всіх plaintext паролів

```
andriy@sos:~$ sudo tcpdump -i any port 443
tcpdump: data link type LINUX_SLL2
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

uname=user&pass=4291231231231
```

d. продемонструвати запити/відповіді до DHCP сервера (як варіант можна скористатися утилітою dhcpdump)

```
DHCPDISCOVER on enp0s3 to 255.255.255.255 port 67 interval 3 (xid=0x7539069)
DHCPOFFER of 10.0.2.15 from 10.0.2.2
DHCPREQUEST for 10.0.2.15 on enp0s3 to 255.255.255.255 port 67 (xid=0x69905307)
DHCPACK of 10.0.2.15 from 10.0.2.2 (xid=0x7539069)
```

3. Встановити Wireshark

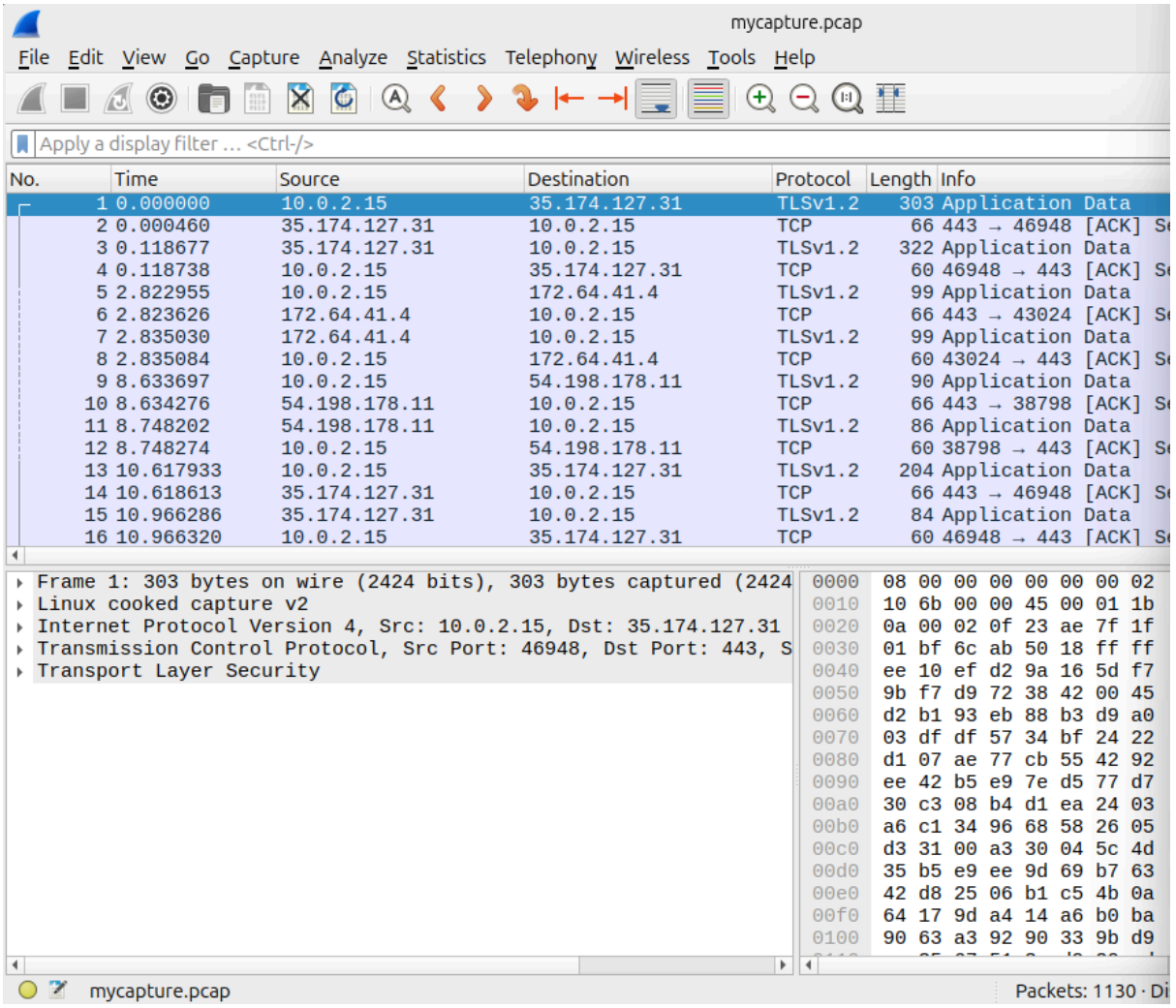
```
andriy@sos:~$ wireshark -h
Wireshark 4.2.2 (Git v4.2.2 packaged as 4.2.2-1.1build3)
Interactively dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: wireshark [options] ... [ <infile> ]

Capture interface:
  -i <interface>, --interface <interface>
                           name or idx of interface (def: first non-loopback)
  -f <capture filter>      packet filter in libpcap filter syntax
  -s <snaplen>, --snapshot-length <snaplen>
                           packet snapshot length (def: appropriate maximum)
  -p, --no-promiscuous-mode
                           don't capture in promiscuous mode
  -I, --monitor-mode       capture in monitor mode, if available
  -B <buffer size>, --buffer-size <buffer size>
                           size of kernel buffer (def: 2MB)
  -y <link type>, --linktype <link type>
                           link layer type (def: first appropriate)
  --time-stamp-type <type> timestamp method for interface
  -D, --list-interfaces    print list of interfaces and exit
  -L, --list-data-link-types
                           print list of link-layer types of iface and exit
```

4. Зробити дамп трафіку за допомогою tcpdump і візуалізувати дані за допомогою Wireshark

```
andriy@sos:~$ sudo tcpdump -i any -w mycapture.pcap
tcpdump: data link type LINUX_SLL2
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot leng
th 262144 bytes
^C1180 packets captured
1273 packets received by filter
0 packets dropped by kernel
```



Висновок: У ході виконання цієї лабораторної роботи я отримав практичний досвід роботи з мережевими протоколами TCP/IP, UDP, ICMP. Ознайомився з функціоналом утиліти tcpdump, яка дозволяє здійснювати перехоплення та аналіз мережевого трафіку. Я навчився фільтрувати пакети, виділяти трафік авторизації, DNS, DHCP, а також виявляти незашифровані паролі в трафіку.

Окрім цього, я встановив Wireshark та навчився працювати з дампами, знятими за допомогою tcpdump, що дозволило більш зручно аналізувати структуру та вміст пакетів. Лабораторна робота допомогла мені краще зрозуміти принципи

функціонування мережевих протоколів та важливість безпечної передачі даних в мережі.