Міністерство освіти і науки України
Львівський національний університет імені Івана Франка
Факультет електроніки та комп’ютерних технологій

Кафедра оптоелектроніки

та інформаційних технологій

Звіт
Про виконання лабораторної роботи №8
З курсу «Комп'ютерні інформаційні мережі»
«Стек протоколів»

Виконав:
Студент групи ФеС-21
Осадчук Дмитро

Львів-2025

ЛАБОРАТОРНА РОБОТА № 8

Тема: Стек протоколів

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

Час виконання: 2 год.

Завдання для виконання:

1. За потреби встановити утиліту tcpdump (https://hackertarget.com/tcpdump-examples/)
2. За допомогою tcpdump
    a. продемонструвати перехоплення авторизаційних даних (логін і пароль) при авторизації в Wordpress
    b. продемонструвати трафік до DNS сервера
    c. продемонструвати перехоплення всіх plaintext паролів
    d. продемонструвати запити/відповіді до DHCP сервера (як варіант можна скористатися утилітою dhcpdump)
3. Встановити Wireshark
4. Зробити дамп трафіку за допомогою tcpdump і візуалізувати дані за допомогою Wireshark
5. Оформити звіт про виконання роботи зі знімками екрана (або його частини), які ілюструють виконання завдань

Хід роботи:

```
xintrea@xintrea-VirtualBox:~$ sudo apt install tcpdump
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tcpdump is already the newest version (4.99.4-3ubuntu4).
tcpdump set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 83 not upgraded.
xintrea@xintrea-VirtualBox:~$
```

Встановив утиліту tcpdump

Результати роботи з tcpdump

```
19:23:01.560731 lo    In  IP localhost.47284 > _localdnsstub.domain: 22848+ [1au] A? detectportal.firefox.com. (53)
19:23:01.561328 lo    In  IP _localdnsstub.domain > localhost.47284: 22848 3/0/2 CNAME detectportal.prod.mozaws.net., CNAME prod
.detectportal.prod.cloudops.mozgcp.net., A 34.107.221.82 (192)
19:23:01.561686 lo    In  IP localhost.47284 > _localdnsstub.domain: 63555+ [1au] AAAA? detectportal.firefox.com. (53)
19:23:01.562122 lo    In  IP _localdnsstub.domain > localhost.47284: 63555 3/0/1 CNAME detectportal.prod.mozaws.net., CNAME prod
.detectportal.prod.cloudops.mozgcp.net., AAAA 2600:1901:0:38d7:: (176)
19:23:01.562642 lo    In  IP localhost.54725 > _localdnsstub.domain: 11639+ [1au] A? detectportal.firefox.com. (53)
19:23:01.563322 lo    In  IP _localdnsstub.domain > localhost.54725: 11639 3/0/2 CNAME detectportal.prod.mozaws.net., CNAME prod
```

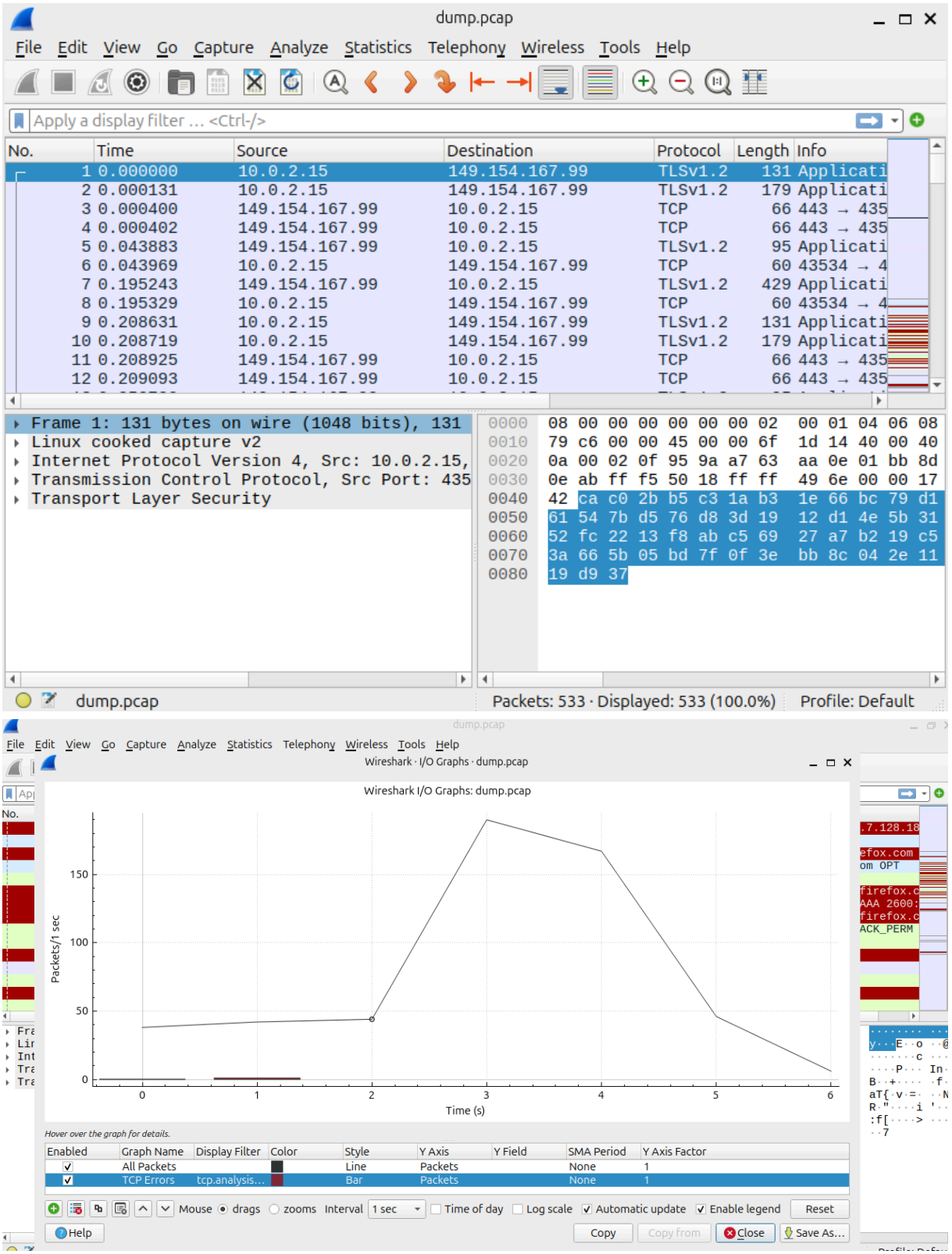
```
19:29:50.546009 enp0s3 In  IP 82.221.107.34.bc.googleusercontent.com.http > xintrea-VirtualBox.53356: Flags [.], ack 9858, win 6
5535, length 0
E..(....@..f"k.R
....P.l..^...j0P...Vl........
19:29:50.547628 enp0s3 Out IP xintrea-VirtualBox.53362 > 82.221.107.34.bc.googleusercontent.com.http: Flags [P.], seq 4515:4816,
 ack 4471, win 63942, length 301: HTTP: GET /canonical.html HTTP/1.1
E..U.=@.@.M.
..."k.R.r.PT#....;2P.......GET /canonical.html HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive


19:29:50.547979 enp0s3 In  IP 82.221.107.34.bc.googleusercontent.com.http > xintrea-VirtualBox.53362: Flags [.], ack 4816, win 6
5535, length 0
E..(....@..d"k.R
....P.r..;2T#..P...aU........
19:29:50.553299 enp0s3 Out IP6 xintrea-VirtualBox.49300 > 2600:1901:0:38d7::.http: Flags [S], seq 2038361905, win 64800, options
```

```
19:31:14.550295 lo    In  IP localhost.32799 > _localdnsstub.domain: 8731+ [1au] AAAA? example.org. (40)
19:31:14.550303 lo    In  IP localhost.41317 > _localdnsstub.domain: 44624+ [1au] AAAA? detectportal.firefox.com. (53)
19:31:14.550690 lo    In  IP _localdnsstub.domain > localhost.44845: 35069 3/0/2 CNAME detectportal.prod.mozaws.net., CNAME prod
.detectportal.prod.cloudops.mozgcp.net., A 34.107.221.82 (192)
19:31:14.550780 lo    In  IP localhost.44845 > _localdnsstub.domain: 38392+ [1au] AAAA? detectportal.firefox.com. (53)
19:31:14.551088 lo    In  IP _localdnsstub.domain > localhost.41317: 65363 3/0/2 CNAME detectportal.prod.mozaws.net., CNAME prod
.detectportal.prod.cloudops.mozgcp.net., A 34.107.221.82 (192)
19:31:14.551484 lo    In  IP _localdnsstub.domain > localhost.32799: 8731 4/0/1 AAAA 2600:1406:bc00:17::6007:810d, AAAA 2600:140
8:ec00:36::1736:7f2e, AAAA 2600:1406:bc00:17::6007:8128, AAAA 2600:1408:ec00:36::1736:7f2f (152)
19:31:14.551789 lo    In  IP _localdnsstub.domain > localhost.41317: 44624 3/0/1 CNAME detectportal.prod.mozaws.net., CNAME prod
.detectportal.prod.cloudops.mozgcp.net., AAAA 2600:1901:0:38d7:: (176)
19:31:14.552174 lo    In  IP _localdnsstub.domain > localhost.44845: 38392 3/0/1 CNAME detectportal.prod.mozaws.net., CNAME prod
.detectportal.prod.cloudops.mozgcp.net., AAAA 2600:1901:0:38d7:: (176)
19:31:14.568161 enp0s3 In  IP 10.0.2.3.domain > xintrea-VirtualBox.52479: 39861 0/1/1 (99)
19:31:14.568513 lo    In  IP _localdnsstub.domain > localhost.41376: 39165 0/1/1 (99)
19:31:14.577151 lo    In  IP localhost.53928 > _localdnsstub.domain: 35962+ [1au] A? ipv4only.arpa. (42)
19:31:14.577261 lo    In  IP localhost.53928 > _localdnsstub.domain: 57212+ [1au] AAAA? ipv4only.arpa. (42)
19:31:14.577600 lo    In  IP _localdnsstub.domain > localhost.53928: 35962 2/0/1 A 192.0.0.170, A 192.0.0.171 (74)
19:31:14.577937 enp0s3 Out IP xintrea-VirtualBox.50158 > 10.0.2.3.domain: 1503+ [1au] AAAA? ipv4only.arpa. (42)
19:31:14.583769 enp0s3 In  IP 10.0.2.3.domain > xintrea-VirtualBox.50158: 1503 0/1/1 (99)
19:31:14.584383 lo    In  IP _localdnsstub.domain > localhost.53928: 57212 0/1/1 (99)
19:31:14.886597 lo    In  IP localhost.44956 > _localdnsstub.domain: 24444+ [1au] A? mozilla.cloudflare-dns.com. (55)
19:31:14.887133 lo    In  IP _localdnsstub.domain > localhost.44956: 24444 2/0/1 A 172.64.41.4, A 162.159.61.4 (87)
19:31:14.887296 lo    In  IP localhost.44956 > _localdnsstub.domain: 32320+ [1au] AAAA? mozilla.cloudflare-dns.com. (55)
19:31:14.887496 lo    In  IP _localdnsstub.domain > localhost.44956: 32320 2/0/1 AAAA 2a06:98c1:52::4, AAAA 2803:f800:53::4 (111
)
```

```
xintrea@xintrea-VirtualBox:~$ sudo usermod -aG wireshark $USER
xintrea@xintrea-VirtualBox:~$ newgrp wireshark
```

Встановлення та налаштування wireshark для роботи



Дамп трафіку та його візуалізація у wireshark

Висновок: під час виконання ЛР-8 я отримав досвід роботи з ICP/IP, UPD, ICMP. Створив “дамп” та навчився його візуалізовувати.