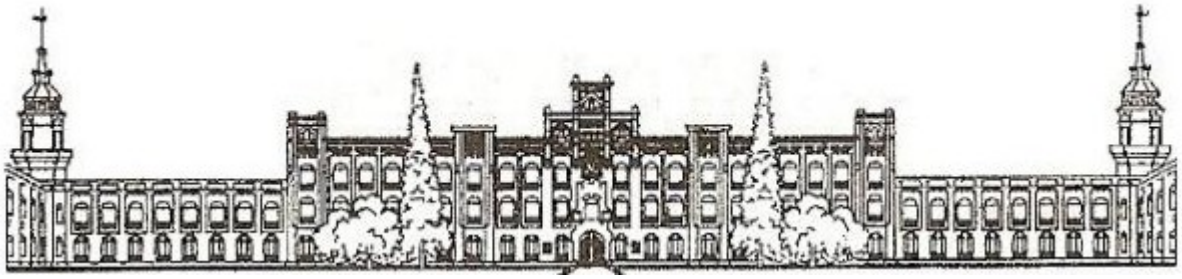

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»

КАФЕДРА ММСА

Лабораторна робота № 1

З дисципліни: Комп’ютерні мережі

Основи захоплення та аналізу пакетів

Виконала:

Студентка III курсу

Групи КА-71

Кравченко А.А.

Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: оволодіти методами роботи в середовищі захоплення та аналізу пакетів.

Хід виконання роботи

Frame 339: 515 bytes on wire (4120 bits), 515 bytes captured (4120 bits) on interface \Device\NPF_{59A8E6A6-5302-4C66-8D5D-71C92005B37A}, id 0

Ethernet II, Src: RealtekU_be:b2:2e (52:54:00:be:b2:2e), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 49853, Dst Port: 80, Seq: 1, Ack: 1, Len: 461

Hypertext Transfer Protocol

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /wireshark-labs/INTRO-wireshark-file1.html

Request Version: HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: uk,ru-UA;q=0.8,ru;q=0.7,en-GB;q=0.5,en-US;q=0.3,en;q=0.2\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18363\r\n

Accept-Encoding: gzip, deflate\r\n

Host: gaia.cs.umass.edu\r\n

Connection: Keep-Alive\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

[HTTP request 1/1]

[Response in frame: 348]

Frame 348: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{59A8E6A6-5302-4C66-8D5D-71C92005B37A}, id 0

Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: RealtekU_be:b2:2e (52:54:00:be:b2:2e)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15

Transmission Control Protocol, Src Port: 80, Dst Port: 49853, Seq: 1, Ack: 462, Len: 438

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Sat, 11 Apr 2020 10:11:12 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Sat, 11 Apr 2020 05:59:04 GMT\r\n

ETag: "51-5a2fd8c159a3c"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 81\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.136336000 seconds]

[Request in frame: 339]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

File Data: 81 bytes

Line-based text data: text/html (3 lines)

Контрольні питання

1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?

   TCP,TLSv1.2, HTTP, ARP, DNS, ICMPv6

   Які протоколи використовувалися в збережених пакетах запиту та відповіді?

   Ethernet II, Internet Protocol Version 4 , TCP

3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?

   Пройшло 0,136336 с.

4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?

Запит:

Вихідна: 10.0.2.15

Цільова: 128.119.245.12

Відповідь:

Вихідний: 128.119.245.12

Цільовий: 10.0.2.15

5. Яким був перший рядок запиту на рівні протоколу HTTP?

   GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

6. Яким був перший рядок відповіді на рівні протоколу HTTP?

   HTTP/1.1 200 OK\r\n

Висновок

В ході виконання даної лабораторної роботи, були набуті навички використання програми Wireshark для захоплення пакетів. Було проаналізовано час за який було відправлено перший запит та отримано першу відповідь, а також було розглянуто протоколи HTTP.