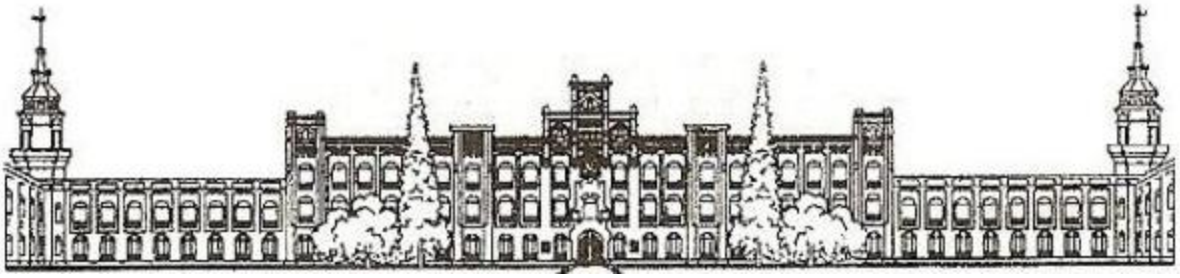

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

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-72

Дунебабіна О.А.

Перевірив: Кухарєв С. О.

Київ 2020

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

Хід виконання роботи

Frame 5: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface \Device\NPF_{AA6559CA-B7D4-4DF0-ACF9-D87205D40E4E}, id 0

Ethernet II, Src: IntelCor_a9:23:ba (28:16:ad:a9:23:ba), Dst: Tp-LinkT_53:b4:1a (84:16:f9:53:b4:1a)

Internet Protocol Version 4, Src: 192.168.0.104, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 56366, Dst Port: 80, Seq: 1, Ack: 1, Len: 485

Hypertext Transfer Protocol

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

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

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0\r\n

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

Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

If-Modified-Since: Tue, 03 Mar 2020 06:59:03 GMT\r\n

If-None-Match: "51-59fedd6cb932e"\r\n

\r\n

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

[HTTP request 1/2]

[Response in frame: 7]

[Next request in frame: 9]

Frame 7: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{AA6559CA-B7D4-4DF0-ACF9-D87205D40E4E}, id 0

Ethernet II, Src: Tp-LinkT_53:b4:1a (84:16:f9:53:b4:1a), Dst: IntelCor_a9:23:ba (28:16:ad:a9:23:ba)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.104

Transmission Control Protocol, Src Port: 80, Dst Port: 56366, Seq: 1, Ack: 486, Len: 438

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Wed, 04 Mar 2020 08:19:42 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: Wed, 04 Mar 2020 06:59:02 GMT\r\n

ETag: "51-5a001f4992162"\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 1/2]

[Time since request: 0.208184000 seconds]

[Request in frame: 5]

[Next request in frame: 9]

[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 - Transmission Control Protocol, HTTP-HyperText Transfer Protocol, DNS - Domain Name System, SSL-Secure Sockets Layer, TLSv1.3 - Transport Layer Security version 1.3, ICMPv6 - , UDP

2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?

   ICP, Ethernet II, HTTP, TCP.

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

Пройшло 0,208184 с.

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

Запит:

Вихідна: 192.168.0.104

Цільова: 128.119.245.12

Відповідь:

Вихідний: 128.119.245.12

Цільовий: 192.168.0.104

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

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

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

HTTP/1.1 200 OK (text/html)

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.