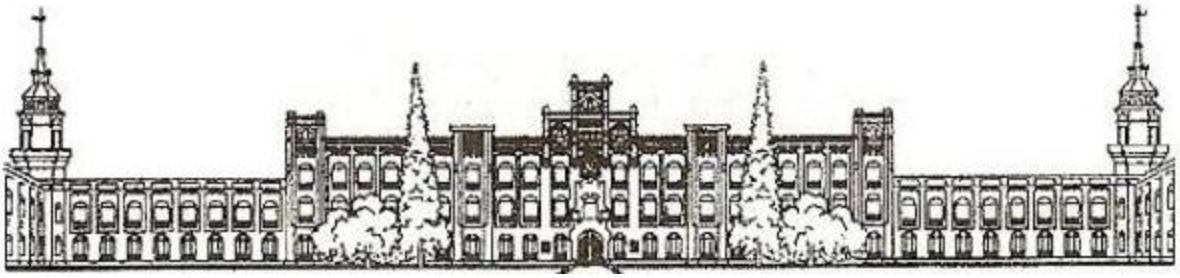

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

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

КАФЕДРА ММСА

Лабораторна робота № 1

З дисципліни: Комп'ютерні мережі

Основи захоплення та аналізу пакетів

Виконав:

Студент III курсу

Групи КА-73

Саакян К.А.

Перевірив: Кухарєв С. О.

Київ 2020

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

Хід виконання роботи

Frame 308: 660 bytes on wire (5280 bits), 660 bytes captured (5280 bits) on interface \Device\NPF_{1DFB6974-4663-4610-BF61-1F6230484D5D}, id 0

Ethernet II, Src: LiteonTe_e6:2b:63 (58:00:e3:e6:2b:63), Dst: 0a:c5:e1:0a:86:9d (0a:c5:e1:0a:86:9d)

Internet Protocol Version 4, Src: 192.168.43.78, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 49175, Dst Port: 80, Seq: 1, Ack: 1, Len: 606

Hypertext Transfer Protocol

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

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

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: uk-UA,uk;q=0.9,ru;q=0.8,en-US;q=0.7,en;q=0.6\r\n

If-None-Match: "51-59f7523c53b13"\r\n

If-Modified-Since: Wed, 26 Feb 2020 06:59:03 GMT\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: 316]

Frame 316: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{1DFB6974-4663-4610-BF61-1F6230484D5D}, id 0

Ethernet II, Src: 0a:c5:e1:0a:86:9d (0a:c5:e1:0a:86:9d), Dst: LiteonTe_e6:2b:63 (58:00:e3:e6:2b:63)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.43.78

Transmission Control Protocol, Src Port: 80, Dst Port: 49175, Seq: 1, Ack: 607, Len: 239

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

Date: Wed, 26 Feb 2020 09:42:14 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

Connection: Keep-Alive\r\n

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

ETag: "51-59f7523c53b13"\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.183602000 seconds]

[Request in frame: 308]

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

Контрольні питання

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

   TCP, HTTP, DNS, SSL, TLSv1.3, 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 0,183602 с.

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

Запит:

Вихідна:129.119.245.12

Цільова:192.168.43.78

Відповідь:

Вихідний: 192.168.43.78

Цільовий: 129.119.245.12

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

GET /favicon.ico HTTP/1.1

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

HTTP/1.1 404 Not Found (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.