МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Лабораторна робота №1

з курсу «Комп’ютерні мережі»

тема: «Основи захоплення та аналізу пакетів»

Виконав: студент 3 курсу

групи КА-77

Науменко В.Є.

Прийняв: Кухарєв С.О.

Київ – 2020р.

Вихідний пакет

No. Time Source Destination Protocol Length Info

787 5.759163 192.168.144.210 128.119.245.12 HTTP 669 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 787: 669 bytes on wire (5352 bits), 669 bytes captured (5352 bits) on interface \Device\NPF_{C8D19F51-CBA9-4481-BAA2-4A68EC151EB4}, id 0

Ethernet II, Src: IntelCor_28:6e:a0 (34:f6:4b:28:6e:a0), Dst: ASUSTekC_67:19:61 (00:18:f3:67:19:61)

Internet Protocol Version 4, Src: 192.168.144.210, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 50243, Dst Port: 80, Seq: 1, Ack: 1, Len: 615

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

DNT: 1\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/80.0.3987.122 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: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7,uk;q=0.6\r\n

If-None-Match: "51-5a001f4992162"\r\n

If-Modified-Since: Wed, 04 Mar 2020 06:59:02 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: 790]

Вихідний пакет

No. Time Source Destination Protocol Length Info

790 5.937841 128.119.245.12 192.168.144.210 HTTP 293 HTTP/1.1 304 Not Modified

Frame 790: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{C8D19F51-CBA9-4481-BAA2-4A68EC151EB4}, id 0

Ethernet II, Src: ASUSTekC_67:19:61 (00:18:f3:67:19:61), Dst: IntelCor_28:6e:a0 (34:f6:4b:28:6e:a0)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.144.210

Transmission Control Protocol, Src Port: 80, Dst Port: 50243, Seq: 1, Ack: 616, Len: 239

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

Date: Wed, 04 Mar 2020 07:51:37 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: "51-5a001f4992162"\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.178678000 seconds]

[Request in frame: 787]

[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?

ARP, TCP, UDP, HTTP, IGMPv2, TLSv1.2, DHCP, SSDP, MDNS

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

Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, Hypertext Transfer Protocol

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

Time =5.937841 – 5.759163 = 0.178678

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

Пакет з запитом:
Вихідна адреса: 192.168.144.210
Цільова адреса: 128.119.245.12

Пакет з відповіддю:
Вихідна адреса: 128.119.245.12
Цільова адреса: 192.168.144.210

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/1.1 304 Not Modified\r\n

Висновки

В ході виконання лабораторної роботи були розглянуті методи роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідні для дослідження мережевих протоколів.