МІНІСТЕРСТВО ОСВІТИ І НАУКИ 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: «Захоплення та аналіз пакетів»

Виконав: студент 3 курсу

групи КА-71

Гікал А.О.

Прийняв: Кухарев С.О.

Київ – 2020р.

No. Time Source Destination Protocol Length Info 122 4.347048 192.168.88.208 128.119.245.12 HTTP 664 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 Frame 122: 664 bytes on wire (5312 bits), 664 bytes captured (5312 bits) on interface \Device\NPF_{C1ABD74C-1A7A-4F73-A39B-50F8232695FA}, id 0 Ethernet II, Src: IntelCor_af:84:7b (fc:77:74:af:84:7b), Dst: Routerbo_35:3a:3d (4c:5e:0c:35:3a:3d) Internet Protocol Version 4, Src: 192.168.88.208, Dst: 128.119.245.12 Transmission Control Protocol, Src Port: 51913, Dst Port: 80, Seq: 1, Ack: 1, Len: 610 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 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/80.0.3987.132 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,en;q=0.9,ru-RU;q=0.8,uk-UA;q=0.7,uk;q=0.6,en-US;q=0.5,de;q=0.4\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: 125]

No. Time Source Destination Protocol Length Info 153 7.118223 128.119.245.12 192.168.88.208 HTTP 293 HTTP/1.1 304 Not Modified Frame 153: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{C1ABD74C-1A7A-4F73-A39B-50F8232695FA}, id 0 Ethernet II, Src: Routerbo_35:3a:3d (4c:5e:0c:35:3a:3d), Dst: IntelCor_af:84:7b (fc:77:74:af:84:7b) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.88.208 Transmission Control Protocol, Src Port: 80, Dst Port: 52095, Seq: 1, Ack: 611, Len: 239 Hypertext Transfer Protocol HTTP/1.1 304 Not Modified\r\n Date: Wed, 04 Mar 2020 08:08:59 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 1/2] [Time since request: 0.220870000 seconds] [Request in frame: 151] [Next request in frame: 155] [Next response in frame: 158] [Request URI: http://gaia.cs.umass.edu/favicon.ico]

Контрольні запитання:

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

UDP, TLSv1.2, TCP, HTTP, DNS.

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

HTTP

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

[Time since request: 0.220870000 seconds]

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

192.168.88.208 128.119.245.12

128.119.245.12 192.168.88.208

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/1.1 304 Not Modified\r\n

Висновки.

Я з’ясував , що програма WireShark дає змогу аналізувати трафік, перехоплювати пакети.