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.

Завдання

1. Запустіть веб-браузер.

2. Запустіть Wireshark.

3. В Wireshark активуйте діалог вибору мережевого інтерфейсу для захоплення: Capture >> Interfaces (або ж Ctrl + I)

4. Далі виберіть той інтерфейс, для якого відображається найбільша кількість захоплених пакетів та натисніть кнопку Start навпроти нього a. в випадку коли інтерфейс ще не ввімкнено можна вибрати any; b. в випадку, коли ви плануєте тестувати локальну комунікацію процесів, можна вибрати lo, loopback або any;

5. Поки Wireshark захоплює пакети, відкрийте в браузері сторінку за наступною адресою: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html Пакети зі вмістом зазначеної веб-сторінки повинні бути захоплені Wireshark.

6. Зупиніть захоплення пакетів за допомогою команди Capture >> Stop (або Ctrl + E)

7. Введіть текст «http» в поле фільтрації та натисніть Apply, в вікні лістингу пакетів мають залишитися тільки пакети, які були створені протоколом HTTP.

8. Виберіть перший пакет HTTP, який відображається в вікні лістингу, це має бути повідомлення GET протоколу HTTP. Також цей пакет має вміщувати інформації інших протоколів нижчих рівнів: TCP, IP, Ethernet.

9. У вікні деталей заголовків розкрийте деталі, пов’язані з протоколом HTTP та скрийте детальну інформацію про інші протоколи.

10. Роздрукуйте перші пакети запиту та відповіді. Для цього слід виділити пакет, який бажано роздрукувати, та активувати команду File > Print, та налаштувати його так як показано на Малюнку 3 (ім’я файлу слід змінити на більш інформативне

11. Перевірте, що у роздрукованих файлах присутні необхідні для захисту пакети та відображені необхідні для захисту протоколу.

12. Закрийте Wireshark.

Вихідний пакет

No. Time Source Destination Protocol Length Info

55 19.110048 192.168.1.104 128.119.245.12 HTTP 673 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 55: 673 bytes on wire (5384 bits), 673 bytes captured (5384 bits) on interface \Device\NPF_{89C98DA1-18B0-437A-ADA6-5872725D58BF}, id 0

Ethernet II, Src: CloudNet_2a:d4:77 (48:5f:99:2a:d4:77), Dst: Tp-LinkT_fe:8b:18 (a0:f3:c1:fe:8b:18)

Internet Protocol Version 4, Src: 192.168.1.104, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 58535, Dst Port: 80, Seq: 1, Ack: 1, Len: 619

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 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36 OPR/66.0.3515.72\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: "51-59eabf95317c3"\r\n

If-Modified-Since: Sun, 16 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: 65]

Вхідний пакет

No. Time Source Destination Protocol Length Info

65 19.240971 128.119.245.12 192.168.1.104 HTTP 293 HTTP/1.1 304 Not Modified

Frame 65: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{89C98DA1-18B0-437A-ADA6-5872725D58BF}, id 0

Ethernet II, Src: Tp-LinkT_fe:8b:18 (a0:f3:c1:fe:8b:18), Dst: CloudNet_2a:d4:77 (48:5f:99:2a:d4:77)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.104

Transmission Control Protocol, Src Port: 80, Dst Port: 58535, Seq: 1, Ack: 620, Len: 239

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

Date: Sun, 16 Feb 2020 14:23:39 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: "51-59eabf95317c3"\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.130923000 seconds]

[Request in frame: 55]

[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, UPD, DNS, HTTP, IGMPv2, TLSv1.2.

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 = 19.240971 – 19.110048 = 0.130923

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

Пакет з запитом:
Вихідна адреса: 192.168.1.104
Цільова адреса: 128.119.245.12

Пакет з відповіддю:
Вихідна адреса: 128.119.245.12
Цільова адреса: 192.168.1.104

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.