Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”

Звіт

про виконання лабороторних робіт
з дисципліни “Комп’ютерні мережі”

Виконав: студент групи ІС-93
Лєпьошкін Є.С.

Лабороторна робота №1

Основи захоплення та аналізу пакетів

Мета роботи: оволодіти методами роботи в середовищі захоплення та аналізу пакетів Wireshark, необхідними для дослідження мережевих протоколів.

Хід роботи:
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).
Малюнок 3. Типові налаштування діалогу роздруківки.
11. Перевірте, що у роздрукованих файлах присутні необхідні для захисту пакети та відображені необхідні для захисту протоколу.
12. Закрийте Wireshark.

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

> ARP, DNS, HTTP, TCP, UDP

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

> HTTP, IPv4, TCP

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

> 0.13 ms

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

> Запит: 192.168.31.178 -> 128.119.245.12
> Відповідь: 128.119.245.12 -> 192.168.31.178

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/1.1 200 OK\r\n

Лабороторна робота №2

Протокол HTTP

Мета роботи: аналіз деталей роботи протоколу HTTP.

Хід роботи:
1. Запустіть веб-браузер, очистіть кеш браузера:
a. для Firefox виконайте
Tools >> Clear Private Data (або Ctrl + Shift + Del)
b. для MS IE виконайте
Tools >> Internet Options >> Delete File
2. Запустіть Wireshark, введіть «http» в поле фільтрації, почніть захоплення пакетів.
3. Відкрийте за допомогою браузера одну із зазначених нижче адрес:
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
http://194.44.29.242/index.html
4. Зупиніть захоплення пакетів.
5. Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім HTTP (за допомогою знаків +/-).
6. Приготуйте відповіді на контрольні запитання 1-7, роздрукуйте необхідні для цього пакети.
7. Почніть захоплення пакетів.
8. Відкрийте у браузері ту ж саму сторінку, або ж просто натисніть F5 для її повторного завантаження.
Якщо ви працюєте зі сторінкою на gaia.cs.umass.edu (ця сторінка регенерується кожну хвилину) – почніть спочатку та виконайте кроки 1,2,3 та 8.
9. Зупиніть захоплення пакетів.
10. Приготуйте відповіді на контрольні запитання 8-11, роздрукуйте необхідні для цього пакети.

11. Віберіть адрес деякого ресурсу (наприклад, зображення), розмір якого перевищує 8192 байти. Можна, наприклад, використати
http://www.dilbert.com/dyn/str_strip/000000000/00000000/0000000/000000/70000/3000/400/73435/73435.strip.gif
http://www.dilbert.com/dyn/str_strip/000000000/00000000/0000000/000000/70000/7000/300/77356/77356.strip.sunday.gif
або будь-який не дуже великий файл з серверу 194.44.29.242.
12. Почніть захоплення пакетів та очистіть кеш браузера.
13. Відкрийте обраний ресурс браузером.
14. Зупиніть захоплення пакетів.
15. Приготуйте відповіді на запитання 12-15. При необхідності роздрукуйте деякі пакети з відповіді сервера.
16. Почніть захоплення пакетів.
17. Відкрийте сторінку за адресою
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
також можна використати будь-яку нескладну сторінку з невеликою кількістю зовнішніх ресурсів.
18. Зупиніть захоплення пакетів.
19. Приготуйте відповіді на запитання 16, 17. Роздрукуйте необхідні для цього пакети.
20. Закрийте Wireshark.

Контрольні запитання:
1. Яку версію протоколу HTTP використовує ваш браузер (1.0 чи 1.1)? Яку версію протоколу використовує сервер?

> 1.1

2. Які мови (якщо вказано) браузер може прийняти від сервера?

> English (en-US)

3. Які IP-адреси вашого комп’ютера та цільового веб-сервера?

> мій комп’ютер: 192.168.31.178
> цільовий: 128.119.245.12

4. Який статусний код сервер повернув у відповіді вашому браузеру?

> 200 OK

5. Коли на сервері в останній раз був модифікований файл, який запитується браузером?

> Sun, 14 Jun 2020 05:59:02 GMT

6. Скільки байт контенту повертається сервером?

> 128 Bytes

7. Переглядаючи нерозібраний байтовий потік пакету, чи бачите ви деякі заголовки в потоці, які не відображаються у вікні деталей пакету? Якщо так, назвіть один з них.

> Всі відображаються

8. Перевірте вміст першого запиту HTTP GET від вашого браузера до сервера. Чи є в ньому заголовок IF-MODIFIED-SINCE?

> Не відображається

9. Перевірте вміст першої відповіді сервера. Чи повернув сервер вміст файлу безпосередньо у відповіді?

> Так повернув

10. Перевірте вміст другого запиту HTTP GET. Чи є в ньому заголовок IF-MODIFIED-SINCE? Якщо так, яке значення йому відповідає?

> If-Modified-Since: Sun, 14 Jun 2020 05:59:02 GMT

11. Який код та опис статусу другої відповіді сервера? Чи повернув сервер вміст файлу безпосередньо у відповіді?

> HTTP/1.1 304 Not Modified\r\n
> Вміст файлу у другому запиті не був поверненний

12. Скільки повідомлень HTTP GET було відправлено вашим браузером?

> 2 GET запита

13. Скільки пакетів TCP було необхідно для доставки одної відповіді HTTP-сервера?

> 2502 пакетів

14. Який код та опис статусу був у відповіді сервера?

> HTTP/1.1 200 OK\r\n

15. Чи зустрічаються у даних пакетів-продовжень протоколу TCP стрічки з кодом та описом статусу відповіді, або ж якісь заголовки протоколу HTTP?

> Відсутні

16. Скільки запитів HTTP GET було відправлено вашим браузером? Якими були цільові IP-адреси запитів?

> Було відравленно 4 GET запити. Цільова адреса була одна: 128.119.245.12

17. Чи можете ви встановити, чи були ресурси отримані паралельно чи послідовно? Яким чином?

> В данному випадку ресурси були отримані послідовно.

Лабороторна робота №3

Протокол DNS

Мета роботи: аналіз деталей роботи протоколу DNS.

Хід роботи:
1. Очистіть кеш DNS-записів
a. для windows-систем виконайте в терміналі
ipconfig /flushdns
b. для linux-систем (можливо) спрацює перезапуск операційної системи;
2. Запустіть веб-браузер, очистіть кеш браузера:
a. для Firefox виконайте
Tools >> Clear Private Data (або Ctrl + Shift + Del)
b. для MS IE виконайте
Tools >> Internet Options >> Delete File
3. Запустіть Wireshark, почніть захоплення пакетів.
4. Відкрийте за допомогою браузера одну із зазначених нижче адрес:
http://www.ietf.org
5. Зупиніть захоплення пакетів.
6. Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім DNS (за допомогою знаків +/-).
7. Приготуйте відповіді на контрольні запитання 1-6, роздрукуйте необхідні для цього пакети.
8. Почніть захоплення пакетів.
9. Виконайте nslookup для домену www.mit.edu за допомогою команди
a. nslookup www.mit.edu
10. Зупиніть захоплення пакетів.
11. Приготуйте відповіді на контрольні запитання 7-10, роздрукуйте необхідні для цього пакети. Утиліта nslookup відправляє три запити та отримує три відповіді, така поведінка є специфічною, тому слід ігнорувати перші два запити та перші дві відповіді.
12. Почніть захоплення пакетів.
13. Виконайте nslookup для домену www.mit.edu за допомогою команди
a. nslookup –type=NS mit.edu14. Зупиніть захоплення пакетів.
15. Приготуйте відповіді на запитання 11-13. При необхідності роздрукуйте деякі захоплені пакети.
16. Почніть захоплення пакетів.

17. Виконайте nslookup для домену www.mit.edu за допомогою команди
a. nslookup www.aiit.or.kr bitsy.mit.edu
18. Зупиніть захоплення пакетів.
19. Приготуйте відповіді на запитання 14-16. При необхідності роздрукуйте деякі захоплені пакети.
20. Закрийте Wireshark.

Контрольні запитання:
1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер вихідного порта відповіді DNS?

> Protocol: UDP, Both ports: 53

2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?

> IP: 192.168.31.1. Це є локальним DNS

3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

> Standard Query - повідомлення є запитом
> Response: Message is a query
Opcode: Standard query (0)
Truncated: Message is not truncated
Recursion desired: Do query recursively
Z: reserved (0)

Queries
www.ietf.org: type A, class IN
Name: www.ietf.org
[Name Length: 12]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 20]

4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?

> Кількість запропонована сервером: 3
> Answers
www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
Name: www.ietf.org
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 300 (5 minutes)

Data length: 33
CNAME: www.ietf.org.cdn.cloudflare.net
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
Name: www.ietf.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 4
Address: 104.20.1.85
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
Name: www.ietf.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 4
Address: 104.20.0.85

5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?

> Так, співпадає. 104.20.1.85

6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які використовує документ, що отримав браузер?

> Так, виконує запит DNS analytics.ietf.org

7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?

> Destination Port: 53, Src Port: 53

8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

> 192.168.31.1 - локальний сервер DNS.

9. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

> Standard Query - повідомлення є запитом
> Domain Name System (query)
Flags: 0x0100 Standard query
Response: Message is a query
Opcode: Standard query (0)
Truncated: Message is not truncated
Recursion desired: Do query recursively
Z: reserved (0)

Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.mit.edu: type A, class IN
Name: www.mit.edu
[Name Length: 11]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 59]

10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей?

> 3 записи.
> Answers
www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
Name: www.mit.edu
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 25
CNAME: www.mit.edu.edgekey.net
www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
Name: www.mit.edu.edgekey.net
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 60 (1 minute)
Data length: 27
CNAME: e9566.dscb.akamaiedge.net
e9566.dscb.akamaiedge.net: type A, class IN, addr 23.7.200.176
Name: e9566.dscb.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 20 (20 seconds)
Data length: 4
Address: 23.7.200.176
> CNAME - канонічне ім'я.
У відповіді отримуємо ланцюг від доменного імені до IP адреси:
www.mit.edu -> www.mit.edu.edgekey.net
www.mit.edu.edgekey.net -> e9566.dscb.akamaiedge.net
e9566.dscb.akamaiedge.net -> 23.7.200.176

11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?

> 192.168.31.1 - локальний сервер DNS.

12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

> Standard Query - повідомлення є запитом
> Domain Name System (query)
Flags: 0x0100 Standard query
Response: Message is a query
Opcode: Standard query (0)
Truncated: Message is not truncated
Recursion desired: Do query recursively
Z: reserved (0)
Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
mit.edu: type NS, class IN
Name: mit.edu
[Name Length: 7]
[Label Count: 2]
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
[Response In: 19]

13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? Які сервери DNS були запропоновані у відповіді? Сервери були запропоновані за допомогою доменного імені, адреси IP або й того й іншого?

> 8 записів.
> Answers
Answers
mit.edu: type NS, class IN, ns eur5.akam.net
mit.edu: type NS, class IN, ns usw2.akam.net
mit.edu: type NS, class IN, ns use5.akam.net
mit.edu: type NS, class IN, ns use2.akam.net
mit.edu: type NS, class IN, ns asia1.akam.net
mit.edu: type NS, class IN, ns asia2.akam.net
mit.edu: type NS, class IN, ns ns1-37.akam.net
mit.edu: type NS, class IN, ns ns1-173.akam.net
> Сервери були запропановані за допомогою доменного імені

14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?

> 18.0.72.3. Не локальна адресою

15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?

> Domain Name System (query)
Transaction ID: 0x1a11
Flags: 0x0100 Standard query
Response: Message is a query
Opcode: Standard query (0)
Truncated: Message is not truncated
Recursion desired: Do query recursively
Z: reserved (0)
Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.aiit.or.kr: type A, class IN
Name: www.aiit.or.kr
[Name Length: 14]
[Label Count: 4]
Type: A (Host Address) (1)
Class: IN (0x0001)

16. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна з цих відповідей?

> 1 запис
> Answers
bitsy.mit.edu: type A, class IN, addr 18.0.72.3
Name: bitsy.mit.edu
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 4
Address: 18.0.72.3