ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

Факультет прикладної математики та інформатики

Комп'ютерні інформаційні мережі

ЛАБОРАТОРНА РОБОТА №7

Виконав :

Ст *Гуменюк С. А.*

ПМІ -33

2024

Тема: Аналіз TCP-сегментів та UDP-датаграм засобами Wireshark

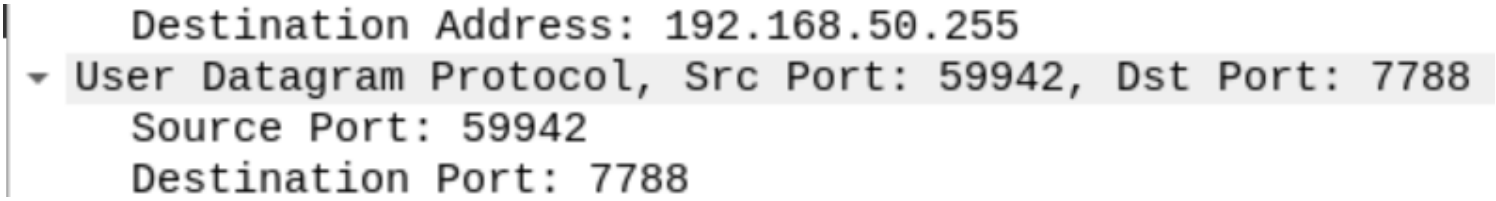
Мета роботи: Здобути практичні навички з інтерпретації протокольних блоків даних транспортного рівня стеку TCP/IP.

Хід роботи

DNS і HTTP відображаються тому, що вони працюють поверх TCP або UDP як транспортних протоколів:

- DNS зазвичай використовує UDP (порт 53)
- HTTP використовує TCP (порт 80/443)

Тобто, коли ми бачимо DNS чи HTTP пакети, вони насправді інкапсульовані в TCP або UDP сегменти, тому і потрапляють під заданий фільтр tcp || udp.

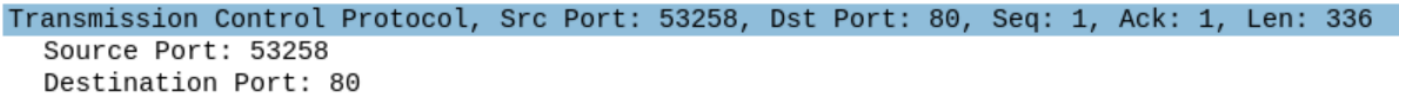


У даному UDP пакеті:

Порт відправника (Source Port): 59942 - цей порт згенерований автоматично операційною системою (динамічний порт)

Порт одержувача (Destination Port): 7788 - цей порт закріплений за конкретним протоколом/сервісом (статичний порт)

Динамічні порти зазвичай генеруються в діапазоні від 49152 до 65535, тому 59942 явно є динамічним портом.



У даному TCP пакеті для HTTP з'єднання:

Порт відправника (Source Port): 53258 - цей порт згенерований автоматично операційною системою (динамічний порт)

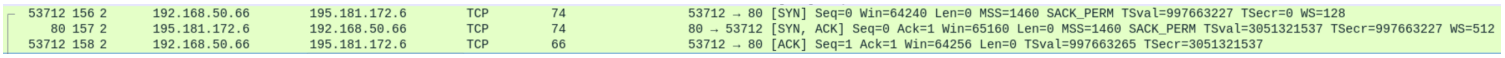
Порт одержувача (Destination Port): 80 - цей порт закріплений за протоколом HTTP (стандартний/статичний порт)

Порт 80 є загальновідомим зарезервованим портом для HTTP протоколу, тоді як 53258 - це динамічний порт, який був автоматично призначений операційною системою для цього з'єднання.

Wireshark відображає HTTPS трафік як "TLSv1.3" (Transport Layer Security) тому, що:

1. HTTPS - це по суті HTTP поверх TLS/SSL шифрування
2. В даному випадку використовується версія протоколу TLS 1.3
3. Wireshark показує TLS замість HTTPS, оскільки пакети зашифровані, і він бачить лише рівень шифрування, а не сам HTTPS протокол

Це можна підтвердити по порту 443, який є стандартним для HTTPS з'єднань.



В процедурі "потрійного рукостискання" TCP:

Перший пакет (SYN):

- Від клієнта (порт 53712) до сервера (порт 80)
- Встановлений прапор SYN
- Початковий номер послідовності (ISN) = 997663227 (справжнє значення)
- Wireshark показує Seq=0 (відносне значення)

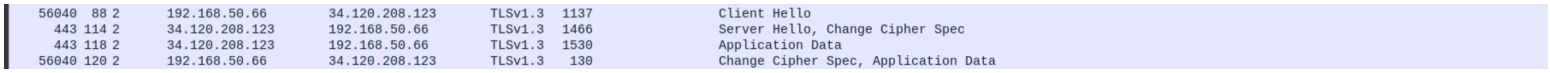
Другий пакет (SYN-ACK):

- Від сервера (порт 80) до клієнта (порт 53712)
- Встановлені прапори SYN і ACK
- Підтверджує отримання першого пакету (ACK = ISN клієнта + 1)
- Має власний початковий номер послідовності (ISN сервера)

Третій пакет (ACK):

- Від клієнта до сервера
- Встановлений прапор ACK
- Підтверджує отримання SYN-ACK від сервера
- Seq = ISN клієнта + 1

Початкові номери послідовності (ISN) генеруються випадково системою для безпеки з'єднання. Wireshark показує відносні значення (починаючи з 0) для спрощення аналізу.



Тут відображається процедура TLS-рукостискання (handshake):

1. Client Hello (від 192.168.50.66):
- Клієнт ініціює TLS з'єднання
- Відправляє список підтримуваних шифрів та параметрів шифрування
- Розмір пакету: 1137 байтів

2. Server Hello, Change Cipher Spec (від 34.120.208.123):
- Сервер відповідає вибором конкретних параметрів шифрування
- Розмір пакету: 1466 байтів

3. Application Data (від 34.120.208.123):
- Передача зашифрованих даних
- Розмір пакету: 1530 байтів

4. Change Cipher Spec, Application Data (від 192.168.50.66):
- Клієнт підтверджує параметри шифрування
- Починається передача зашифрованих даних
- Розмір пакету: 130 байтів

Це стандартна послідовність встановлення захищеного TLS з'єднання.