Тема роботи: Дослідження передавання пакетів у мережі за допомогою програми WireShark.

Мета роботи: Дослідити вміст мережевих пакетів та визначити основні параметри які відповідають рівням моделі OSI.

ТЕОРЕТИЧНІ ВІДОМОСТІ

ХІД РОБОТИ

1) Відкрийте програму WireShark та розпочніть захоплення пакетів. Для цього виберіть локальний мережевий адаптер та двічі на нього натисніть.

2) Відкрийте командну стрічку CMD (Win+R та введіть cmd). У вікні що з'явилось виконайте команду **`ping 8.8.8.8`** та перейдіть назад до програми WireShark. У полі *Filter* введіть значення *ICMP* та натисніть Enter.

   a) Скільки пакетів було захоплено при виконання однієї команди *ping*?

   b) Виберіть перший захоплений пакет (у полі Info вказано що це *request*). Яка IP адреса джерела відправлення? Яка адреса призначення?

3) Двічі натисніть на перший пакет (відкриється вікно з інформацією про структуру пакету):

   a) Розгорніть вкладку для *Internet Control Message Protocol* та вкажіть який тип даного пакету?

   b) Розгорніть вкладку для *Internet Protocol*. Порівняйте присутні поля із тими що відображались у програмі Cisco Packet Tracer. Скільки та які Прапорці (flags) є у IP пакеті?

   c) Розгорніть вкладку *Ethernet II*. Вкажіть яка MAC адреса джерела та призначення?

   d) Розгорніть останню вкладку (Frame). Прослідкуйте процес інкапсуляції даних у полі *Protocols in frame* та вкажіть тип інкапсуляції (*Encapsulation type*).

   e) Повторіть вище описані кроки з пакетом відповіддю (*reply*).

4) Перейдіть у командну стрічку та виконайте команду **`nslookup vns.lpnu.ua`**

   a) Визначте яка IP адреса сайту ВНС?

5) Зайдіть у браузер та у стрічці URL вкажіть IP адресу отриману у попередньому пункті. Перейдіть у WireShark та відфільтруйте пакети згідно отриманої IP адреси сайту ВНС ввівши у поле фільтра **`ip.addr ==`** *Знайдена IP адреса*. Виберіть перший захоплений пакет та натисніть праву клавішу миші. Виберіть пункт Follow -> TCP Stream

   a) Вкажіть яка версія протоколу HTTP використовується?

   b) У вікні що відкрилось знайдіть значення *User-agent*?

   c) Вкажіть характеристики сервера до якого здійснено з'єднання?

6) Верніться до головного вікна WireShark і у полі фільтра допишіть **`and tcp.seq == 0`** . Після застосування фільтра виберіть перший пакет (переконайтесь що *seq=0*) та розгорніть вкладку *Transmission control protocol*.

   a) Визначте значення *Source and Destinatin Port*?

   b) Визначте який встановлений прапорець (Flags). Що означає це значення?

   c) Вкажіть значення *Window Size*. Що означає це значення?

   d) Виберіть наступний пакет з вікна WireShark (пакет відповідь) та дослідіть поле прапорці (Flags). Чому тепер встановлено 2 прапорці?

7) Видаліть попередній фільтр однак залиште фільтрування по IP адресі. Введіть додатковий фільтр **`and http`** та виберіть перший пакет.

   a) Виберіть вкладку *Hyper text protocol* та визначте яка версія HTTP використовується?

   b) Визначте значення *Host* та *User-agent*?