**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»**

**Кафедра Телекомунікації**

|  |  |
| --- | --- |
| **Робота №** | 2 |
| **Група** | ТР-34 |
| **Студент** | Кость В.І. |
| **Викладач** | Данильченко Т.Є. |

|  |  |
| --- | --- |
| **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. |
| **Завдання:** | Виконати завдання згідно ходу роботи.  Дати відповіді на питання під час виконання завдань. |
| **Результат виконаної роботи:** | - При виконанні команди « ping » було захоплено 8 пакетів.  - В першому захопленому пакеті було :  \* ІР адреса джерела відправлення :192.168.75.171  \* ІР адреса призначення : 8.8.8.8  - В Internet Control Message Protocol ми дізналися тип даного пакета :  \* Type: 8 (Echo (ping) request)  - В Internet Protocol ми побачили скільки та які прапорці є у ІР пакеті:  \* в Cisco Packet Tracer 0x0, a y Wireshark 0x0000.  - У вкладці Ethernet II ми дізнались МАС адресу:  \* МАС адреса джерела 74:40:bb:b7:d5:1b  \* МАС адреса призначення 00:1e:bd:21:23:00  - У вкладці Frame ми дізнались тип інкапсуляції :  \* eth:ethertype:ip:icmp:data  - У другому захопленому пакеті було :  \* ІР адреса джерела відправлення : 8.8.8.8  \* ІР адреса призначення : 192.168.75.171  - В Internet Control Message Protocol ми дізналися тип даного пакета :  \* Type: 0 (Echo (ping) request)  - В Internet Protocol ми побачилт скільки та які Прапорці є у ІР пакеті:  \* в Cisco Packet Tracer 0x0, a y Wireshark 0x0000.  - У вкладці Ethernet II ми дізнались МАС адреса:  \* МАС адреса джерела 74:40:bb:b7:d5:1b  \* МАС адреса призначення 00:1e:bd:21:23:00  - У вкладці Frame ми дізнались тип інкапсуляції :  \* eth:ethertype:ip:icmp:data  - Перейшовши у командну стрічку та виконавши команду nslookup vns.lpnu.ua ми визначили ІР адрес ВНС :195.22.112.13  - Ми продовжили дослідження пакетів по ІР адресу ВНС де визначили:  \* Версію протоколу : HTTP/ 1.1  \* User-agent : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 YaBrowser/19.3.0.2485 Yowser/2.5 Safari/537.36  \* Характеристики сервера до якого здійснено з’єднання: Apache/2.4.27 (Red Hat) PHP/7.0.27  -Після застосування фільтру з додаванням and tcp.seq == 0 ми відкриваємо перший пакет досліджуємо вкладку Transmission control protocol :  \* Source Port: 57096.  \* Destinatin Port: 80  \* У нас встановлений flags : 0х002 (SYN)  \* Window Size : 64240  - У пакеті відповідь y нас уже є два прапорці : flags : 0х012 (SYN,ACK)  - Залишивши фільтр по ІР адресі та добавивши фільтр and http ми досліджуєм перший пакет  \* Версію протоколу : HTTP /1.1\r\n  \* Host : 195.22.112.13\r\n  \* User-agent : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 YaBrowser/19.3.0.2485 Yowser/2.5 Safari/537.36 |
| **Висновок:** | Я навчився використовувати програму WireShark для дослідження вмісту мережевих пакетів. Отримано навички захоплення пакетів та використання різних функцій програми WireShark. |