МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ

Протокол

Лабораторна робота №4

На тему: “Дослідження локальних мереж. Використання Wireshark”

Виконав:
Студент групи
АМ-182
Борщов М. І.
Перевірила:
Шапоріна О.Л.

2021

Мета роботи: Навчитися здійснювати аналіз трафіку між пристроями мережі

Завдання:

1. За допомогою програми Nmap визначити наявні хости та сервіси в мережі.

2. Провести пінгування одного з активних хостів мережі. Дослідити процес пошуку фізичної адреси пристрою. Визначити, які протоколи використовувались в даному процесі та провести фільтацію за кожним з них. Дослідити зміст відповідних мережних пакетів. Результат аналізу повинен містити поетапний детальних звіт про транзакції на інтерфейсі, починаючи з генерації пінг-процесу до відповіді відповідного пристрою.

3. Визначити будь-який пакет даних, який містить записи про використання протоколу рівня додатків. Достдідити зміст даного пакети. Відслідкувати дані, які асоційовані з даним пакетом.

Хід роботи

1. Пошук робочих станцій у локальній мережі:

```
nmap -sN 192.168.0.1/24

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-30 19:38 FLE Daylight Time
Nmap scan report for 192.168.0.1
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.0.1 are open|filtered
MAC Address: 74:DA:88:D9:F8:4F (Tp-link Technologies)

Nmap scan report for 192.168.0.100
Host is up (0.066s latency).
All 1000 scanned ports on 192.168.0.100 are open|filtered
MAC Address: 5C:C1:D7:9E:3E:72 (Samsung Electronics)

Nmap scan report for 192.168.0.101
Host is up (0.066s latency).
All 1000 scanned ports on 192.168.0.101 are open|filtered
MAC Address: 68:27:37:B2:B3:E0 (Samsung Electronics)

Nmap scan report for 192.168.0.104
Host is up (0.057s latency).
All 1000 scanned ports on 192.168.0.104 are closed
MAC Address: A4:45:19:5B:36:94 (Xiaomi Communications)

Nmap scan report for 192.168.0.105
Host is up (0.068s latency).
All 1000 scanned ports on 192.168.0.105 are open|filtered
MAC Address: 74:E5:F9:EB:C8:E6 (Intel Corporate)

Nmap scan report for 192.168.0.107
Host is up (0.19s latency).
All 1000 scanned ports on 192.168.0.107 are closed
MAC Address: 42:11:1C:76:6A:DA (Unknown)

Nmap scan report for 192.168.0.116
Host is up (0.035s latency).
All 1000 scanned ports on 192.168.0.116 are closed
MAC Address: D0:28:BA:3D:B1:13 (Realme Chongqing MobileTelecommunications)

Nmap scan report for 192.168.0.117
Host is up (0.10s latency).
All 1000 scanned ports on 192.168.0.117 are open|filtered
MAC Address: 38:A4:ED:6D:F4:5D (Xiaomi Communications)

Nmap scan report for 192.168.0.118
Host is up (0.090s latency).
All 1000 scanned ports on 192.168.0.118 are open|filtered
MAC Address: 00:23:15:76:08:F4 (Intel Corporate)


Nmap scan report for 192.168.0.115
Host is up (0.00039s latency).
All 1000 scanned ports on 192.168.0.115 are closed

Nmap done: 256 IP addresses (10 hosts up) scanned in 222.99 seconds
```

2. Обраний адрес для пінгування 192.168.116

```
C:\Users\nicko>ping 192.168.0.116

Pinging 192.168.0.116 with 32 bytes of data:
Reply from 192.168.0.116: bytes=32 time=73ms TTL=64
Reply from 192.168.0.116: bytes=32 time=94ms TTL=64
Reply from 192.168.0.116: bytes=32 time=2ms TTL=64
Reply from 192.168.0.116: bytes=32 time=28ms TTL=64

Ping statistics for 192.168.0.116:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 94ms, Average = 49ms

C:\Users\nicko>
```

3.

Фільтрація ARP-протокола

arp

No.	Time	Source	Destination	Protocol	Length	Info
108	0.401851	IntelCor_76:08:f4	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.118
2521	5.555345	Tp-LinkT_d9:f8:4f	IntelCor_07:13:d1	ARP	42	Who has 192.168.0.115? Tell 192.168.0.1
2522	5.555361	IntelCor_07:13:d1	Tp-LinkT_d9:f8:4f	ARP	42	192.168.0.115 is at c8:e2:65:07:13:d1
4281	10.435640	IntelCor_76:08:f4	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.118
6059	15.760852	XiaomiCo_6d:f4:5d	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.117
7647	20.470094	IntelCor_76:08:f4	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.118

Фільтрація ICMP-протокола

icmp

No.	Time	Source	Destination	Protocol	Length	Info
5458	16.212997	192.168.0.115	192.168.0.116	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (reply in 5459)
5459	16.214898	192.168.0.116	192.168.0.115	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl=64 (request in 5458)
5712	17.216264	192.168.0.115	192.168.0.116	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 5751)
5751	17.365901	192.168.0.116	192.168.0.115	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=64 (request in 5712)
6009	18.220552	192.168.0.115	192.168.0.116	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 6040)
6040	18.290816	192.168.0.116	192.168.0.115	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=64 (request in 6009)
6521	19.226068	192.168.0.115	192.168.0.116	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 6584)
6584	19.316036	192.168.0.116	192.168.0.115	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=64 (request in 6521)

ICMP-протокол посилає запрос до робочої станції

ARP-протокол потрібен для визначення MAC-адресу

Зміст ARP-вопроса

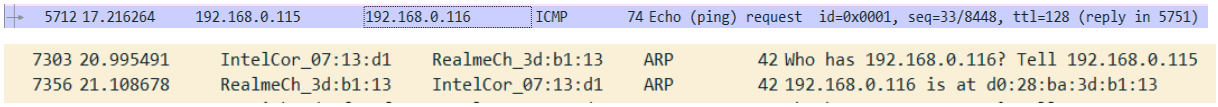
```
> Frame 42705: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{276F8115-BC2C-4BB4-BB02-F2B577BF511D}, id
v Ethernet II, Src: Tp-LinkT_d9:f8:4f (74:da:88:d9:f8:4f), Dst: IntelCor_07:13:d1 (c8:e2:65:07:13:d1)
  v Destination: IntelCor_07:13:d1 (c8:e2:65:07:13:d1)
      Address: IntelCor_07:13:d1 (c8:e2:65:07:13:d1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Tp-LinkT_d9:f8:4f (74:da:88:d9:f8:4f)
      Address: Tp-LinkT_d9:f8:4f (74:da:88:d9:f8:4f)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Tp-LinkT_d9:f8:4f (74:da:88:d9:f8:4f)
    Sender IP address: 192.168.0.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.0.115
```

Зміст ARP-відповіді

```
> Frame 42706: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{276F8115-BC2C-4BB4-BB02-F2B577BF511D}, id 0
v Ethernet II, Src: IntelCor_07:13:d1 (c8:e2:65:07:13:d1), Dst: Tp-LinkT_d9:f8:4f (74:da:88:d9:f8:4f)
  v Destination: Tp-LinkT_d9:f8:4f (74:da:88:d9:f8:4f)
      Address: Tp-LinkT_d9:f8:4f (74:da:88:d9:f8:4f)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: IntelCor_07:13:d1 (c8:e2:65:07:13:d1)
      Address: IntelCor_07:13:d1 (c8:e2:65:07:13:d1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: IntelCor_07:13:d1 (c8:e2:65:07:13:d1)
    Sender IP address: 192.168.0.115
    Target MAC address: Tp-LinkT_d9:f8:4f (74:da:88:d9:f8:4f)
    Target IP address: 192.168.0.1
```

Зміст ICMP-протокола до адреси 192.168.0.116

```
> Frame 5712: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{276F8115-BC2C-4BB4-BB02-F2B577BF511D}, id 0
v Ethernet II, Src: IntelCor_07:13:d1 (c8:e2:65:07:13:d1), Dst: RealmeCh_3d:b1:13 (d0:28:ba:3d:b1:13)
  v Destination: RealmeCh_3d:b1:13 (d0:28:ba:3d:b1:13)
      Address: RealmeCh_3d:b1:13 (d0:28:ba:3d:b1:13)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: IntelCor_07:13:d1 (c8:e2:65:07:13:d1)
      Address: IntelCor_07:13:d1 (c8:e2:65:07:13:d1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.0.115, Dst: 192.168.0.116
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x1541 (5441)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.115
    Destination Address: 192.168.0.116
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d3a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 33 (0x0021)
    Sequence Number (LE): 8448 (0x2100)
    [Response frame: 5751]
  > Data (32 bytes)
```



Спершу за допомогою протоколу ICMP відправляється запрос до потрібного IP-адресу, після цього за допомогою протоколу ARP шукається MAC-адреса пристрою по заданому IP-адресу, після чого отримує MAC-адресу потрібного пристрою (протокол ARP).

Висновок. Було проведено аналіз трафіку у локальній мережі, були досліджені протоколі ARP та ICMP, навчився шукати фізичну адресу потрібної робочої станції, та проаналізовано данні з пакетів.