



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ

СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра Інформаційної Безпеки

Аналіз та моніторинг кібербезпеки

Практичне завдання №3

Моніторинг мережевої активності в ІТС

Перевірів:

Козленко О. В.

Виконав:

студент IV курсу

групи ФБ-01

Сахній Н. Р.

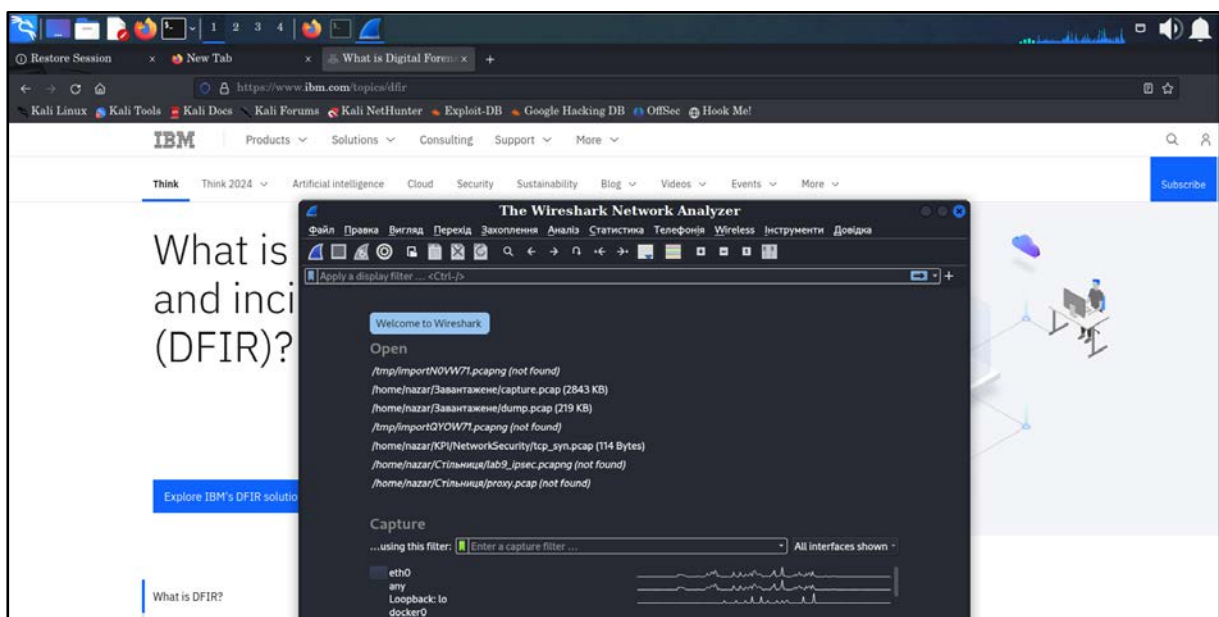
Київ 2024

Мета: Здобуття практичних навичок збору та аналізу мережевого трафіку.

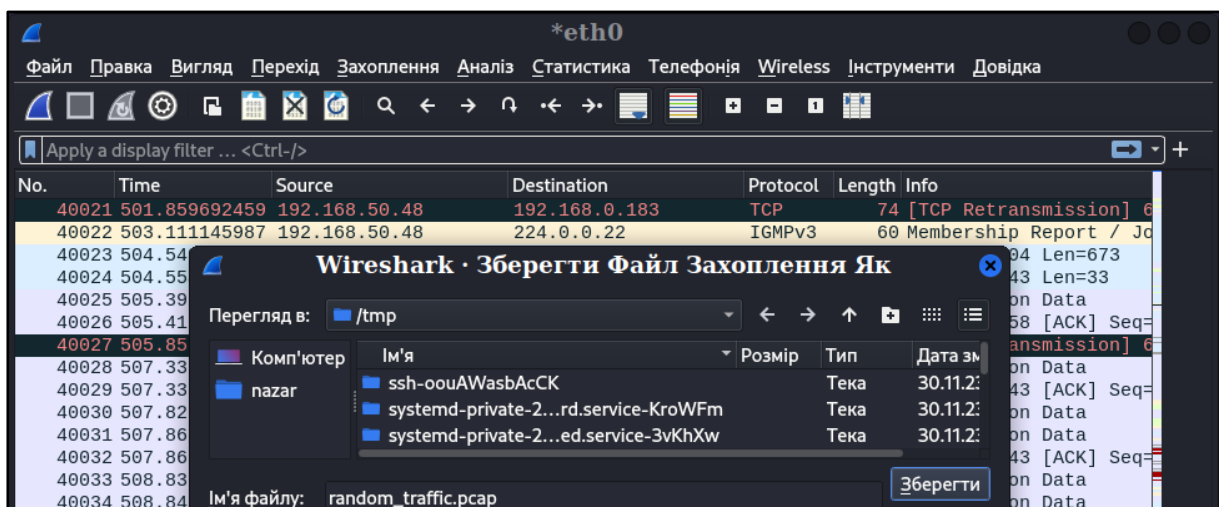
Завдання: Проаналізувати файл захоплення мережевого трафіку за допомогою Xplico, зробити звіт.

❖ Перехоплення мережевого трафіку за допомогою Wireshark

1. Запустимо процес перехоплення трафіку по мережі:



2. Збережемо цей весь трафік до файлу із розширенням “**.pcap**”:



❖ Встановлення Xplico та запуск бази даних

1. Спробуємо завантажити Xplico та запустити одразу ж apache2:

```
(nazar@snz24)-[~]
$ sudo apt-get install xplico
Зчитування переліків пакунків ... Виконано
Побудова дерева залежностей ... Виконано
Зчитування інформації про стан ... Виконано
xplico is already the newest version (1.2.2-0kali6).
оновлено 0, встановлено 0 нових, 0 відмічено для видалення і 2195 не оновлено.
```

```
(nazar@snz24)-[~]
$ sudo systemctl start apache2

(nazar@snz24)-[~]
$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Wed 2024-02-14 19:57:04 EET; 14s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 978142 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 978166 (apache2)
      Tasks: 6 (limit: 4599)
     Memory: 23.5M
        CPU: 208ms
    CGroup: /system.slice/apache2.service
           └─978166 /usr/sbin/apache2 -k start
             └─978176 /usr/sbin/apache2 -k start
               └─978177 /usr/sbin/apache2 -k start
                 └─978178 /usr/sbin/apache2 -k start
                   └─978179 /usr/sbin/apache2 -k start
                     └─978180 /usr/sbin/apache2 -k start

лют 14 19:57:03 snz24 systemd[1]: Starting apache2.service - The Apache HTTP Server ...
лют 14 19:57:04 snz24 apachectl[978165]: AH00558: apache2: Could not reliably determine the server
лют 14 19:57:04 snz24 systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-20/20 (END)
```

2. Запустимо базу даних для її виконання у фоновому режимі:

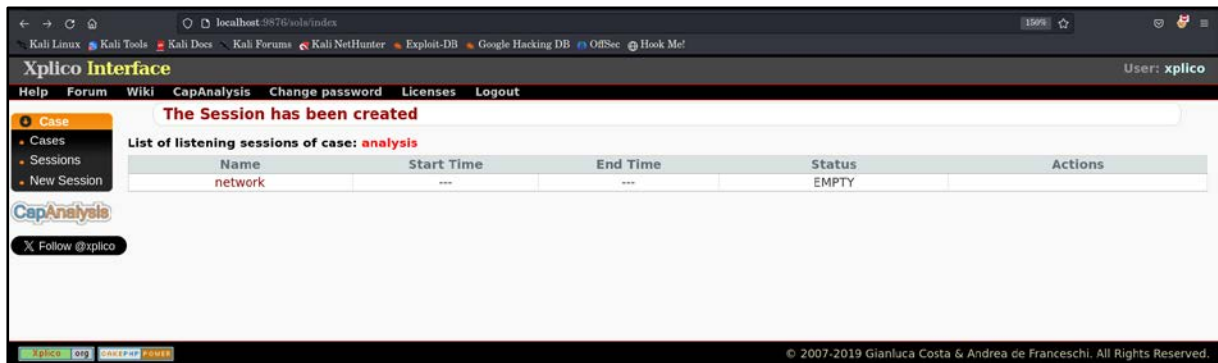
```
(nazar@snz24)-[~]
$ sudo /etc/init.d/xplico start
Starting xplico (via systemctl): xplico.service.

(nazar@snz24)-[~]
$ sudo /etc/init.d/xplico status
● xplico.service - Xplico
   Loaded: loaded (/lib/systemd/system/xplico.service; disabled; preset: disabled)
   Active: active (running) since Wed 2024-02-14 19:58:10 EET; 6s ago
     Docs: https://www.xplico.org/docs
  Process: 978760 ExecStart=/opt/xplico/bin/dema -d /opt/xplico -b sqlite (code=exited, status=0/SUCCESS)
    Main PID: 978761 (dema)
      Tasks: 1 (limit: 4599)
     Memory: 4.4M
        CPU: 67ms
    CGroup: /system.slice/xplico.service
           └─978761 /opt/xplico/bin/dema -d /opt/xplico -b sqlite

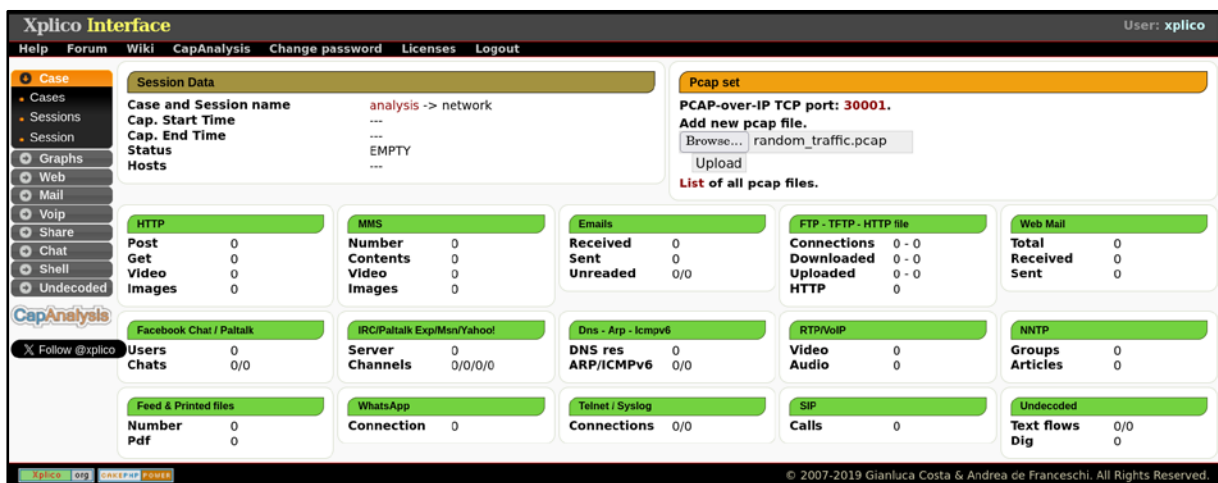
Feb 14 19:58:10 snz24 systemd[1]: Starting xplico.service - Xplico ...
Feb 14 19:58:10 snz24 systemd[1]: xplico.service: Can't open PID file /run/dema.pid (yet?) after start
Feb 14 19:58:10 snz24 systemd[1]: Started xplico.service - Xplico.
```

❖ Аналіз (парсинг) файлу перехопленого трафіку

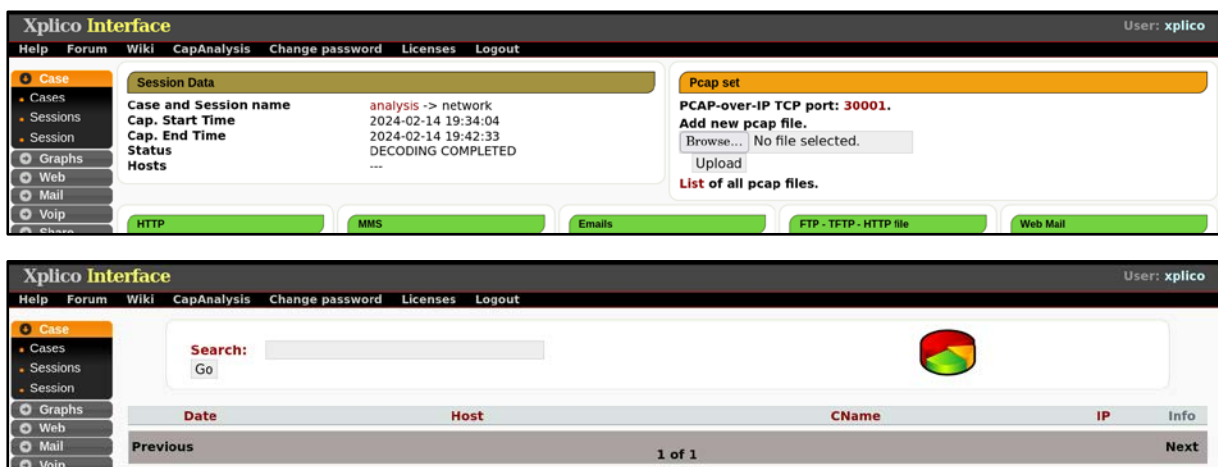
1. Додамо новий сеанс в попередньо створеній новій справі:



2. Завантажимо файл мережевого перехоплення та запустимо декодування:

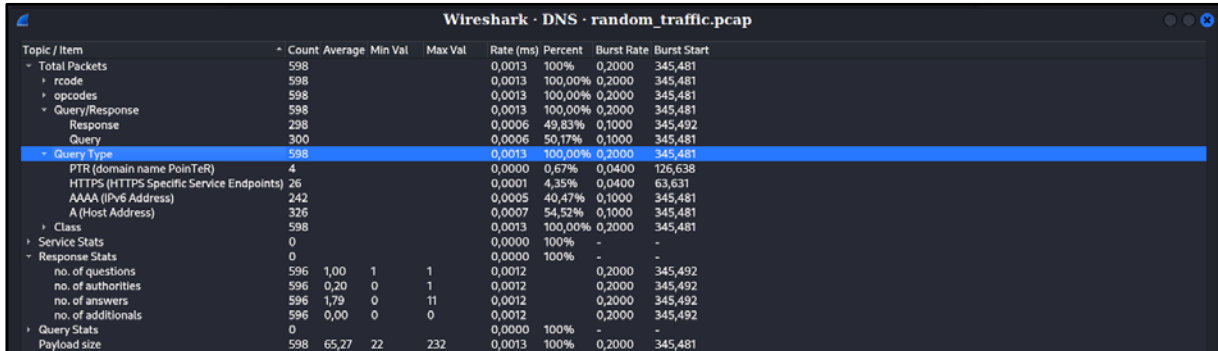


3. Бачимо, що інформація про будь-які мережеві комунікації відсутня:



* Додатковий перегляд статистики по трафіку у Wireshark

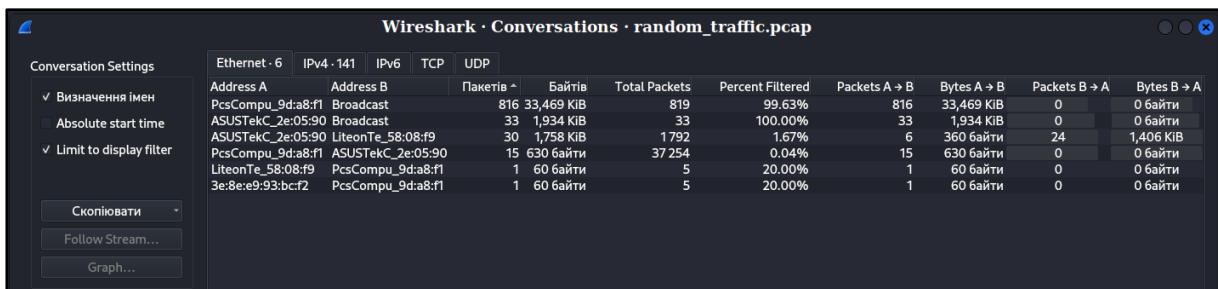
1. Найбільша к-ть DNS-запитів здійснювалась до А-записів (Host Address):



Wireshark - DNS - random_traffic.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total Packets	598				0,0013	100%	0,2000	345,481
rcode	598				0,0013	100,00%	0,2000	345,481
opcodes	598				0,0013	100,00%	0,2000	345,481
Query/Response	598				0,0013	100,00%	0,2000	345,481
Response	298				0,0006	49,83%	0,1000	345,492
Query	300				0,0006	50,17%	0,1000	345,481
Query type	598				0,0013	100,00%	0,2000	345,481
PTR (domain name PointeR)	4				0,0000	0,67%	0,0400	126,638
HTTPS (HTTPS Specific Service Endpoints)	26				0,0001	4,35%	0,0400	63,631
AAAA (IPv6 Address)	242				0,0005	40,47%	0,1000	345,481
A (Host Address)	326				0,0007	54,52%	0,1000	345,481
Class	598				0,0013	100,00%	0,2000	345,481
Service Stats	0				0,0000	100%	-	-
Response Stats	0				0,0000	100%	-	-
no. of questions	596	1,00	1	1	0,0012		0,2000	345,492
no. of authorities	596	0,20	0	1	0,0012		0,2000	345,492
no. of answers	596	1,79	0	11	0,0012		0,2000	345,492
no. of additionals	596	0,00	0	0	0,0012		0,2000	345,492
Query Stats	0				0,0000	100%	-	-
Payload size	598	65,27	22	232	0,0013	100%	0,2000	345,481

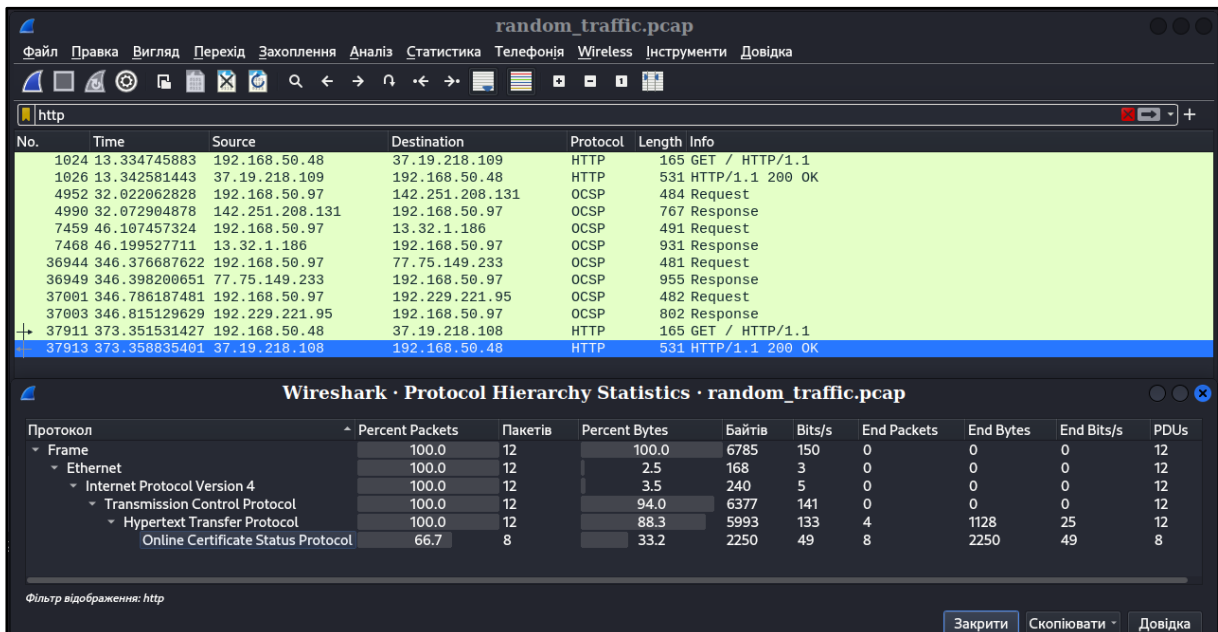
2. Список MAC-адрес, із якими виконувались взаємодія по протоколу ARP:



Wireshark - Conversations - random_traffic.pcap

Conversation Settings	Ethernet - 6	IPv4 - 141	IPv6	TCP	UDP	Address A	Address B	Пакетів	Байтів	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
✓ Визначення імен						PcsCompu_9d:a8:f1	Broadcast	816	33,469 KIB	816	99,63%	816	33,469 KIB	0	0 байти
Absolute start time						ASUSTekC_2e:05:90	Broadcast	33	1,934 KIB	33	100,00%	33	1,934 KIB	0	0 байти
✓ Limit to display filter						ASUSTekC_2e:05:90	LiteonTe_58:08:f9	30	1,758 KIB	1792	1,67%	6	360 байти	24	1,406 KIB
						PcsCompu_9d:a8:f1	ASUSTekC_2e:05:90	15	630 байти	37,254	0,04%	15	630 байти	0	0 байти
						LiteonTe_58:08:f9	PcsCompu_9d:a8:f1	1	60 байти	5	20,00%	1	60 байти	0	0 байти
						3e:8e:e9:93:bcf2	PcsCompu_9d:a8:f1	1	60 байти	5	20,00%	1	60 байти	0	0 байти

3. Ієрархія протоколів під час комунікацій із веб-застосунками в інтернеті:



random_traffic.pcap

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти Довідка

http

No.	Time	Source	Destination	Protocol	Length	Info
1024	13.334745883	192.168.50.48	37.19.218.109	HTTP	165	GET / HTTP/1.1
1026	13.342581443	37.19.218.109	192.168.50.48	HTTP	531	HTTP/1.1 200 OK
4952	32.022062828	192.168.50.97	142.251.208.131	OCSP	484	Request
4990	32.072904878	142.251.208.131	192.168.50.97	OCSP	767	Response
7459	46.107457324	192.168.50.97	13.32.1.186	OCSP	491	Request
7468	46.199527711	13.32.1.186	192.168.50.97	OCSP	931	Response
36944	346.376687622	192.168.50.97	77.75.149.233	OCSP	481	Request
36949	346.398200651	77.75.149.233	192.168.50.97	OCSP	955	Response
37001	346.786187481	192.168.50.97	192.229.221.95	OCSP	482	Request
37003	346.815129629	192.229.221.95	192.168.50.97	OCSP	802	Response
37911	373.351531427	192.168.50.48	37.19.218.108	HTTP	165	GET / HTTP/1.1
37913	373.358835401	37.19.218.108	192.168.50.48	HTTP	531	HTTP/1.1 200 OK

Wireshark - Protocol Hierarchy Statistics - random_traffic.pcap

Протокол	Percent Packets	Пакетів	Percent Bytes	Байтів	Bits/s	End Packets	End Bytes	End Bits/s	PDU's
Frame	100.0	12	100.0	6785	150	0	0	0	12
Ethernet	100.0	12	2.5	168	3	0	0	0	12
Internet Protocol Version 4	100.0	12	3.5	240	5	0	0	0	12
Transmission Control Protocol	100.0	12	94.0	6377	141	0	0	0	12
Hypertext Transfer Protocol	100.0	12	88.3	5993	133	4	1128	25	12
Online Certificate Status Protocol	66.7	8	33.2	2250	49	8	2250	49	8

Фільтр відображення: http

Закрити Скопіювати Довідка