МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Управління кіберінцидентами та аналіз подій»

**Тема № 2**. Електронна комунікаційна мережа об’єкта кіберзахисту як джерело ознак кіберінциденту.

**Заняття № 2/6.** Технологічні основи реєстрації подій в каналі електронної комунікації з використанням tcpdump.

**TCPDUMP, РОЗРОБЛЕННЯ ПРАВИЛ РЕЄСТРАЦІЇ ПОДІЙ**

**Виконав:** курсант навчальної групи 314

ст.солдат \_\_\_\_\_\_\_\_\_\_\_\_\_ Буховцев Г.І.

05.04.2024

**Перевiрив:** викладач кафедри № 33

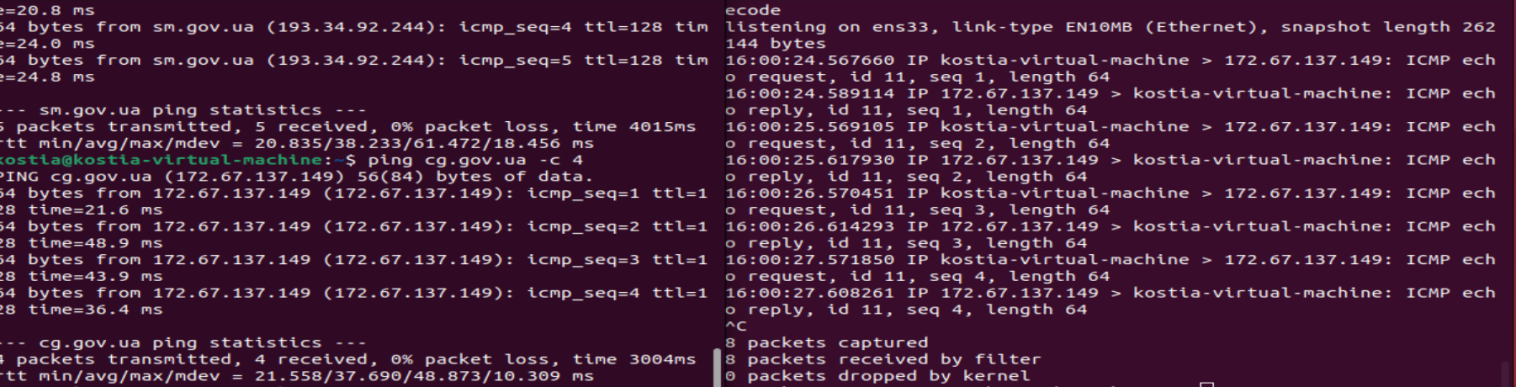
капітан\_\_\_\_\_\_\_ Прийма О.О.

Київ – 2024

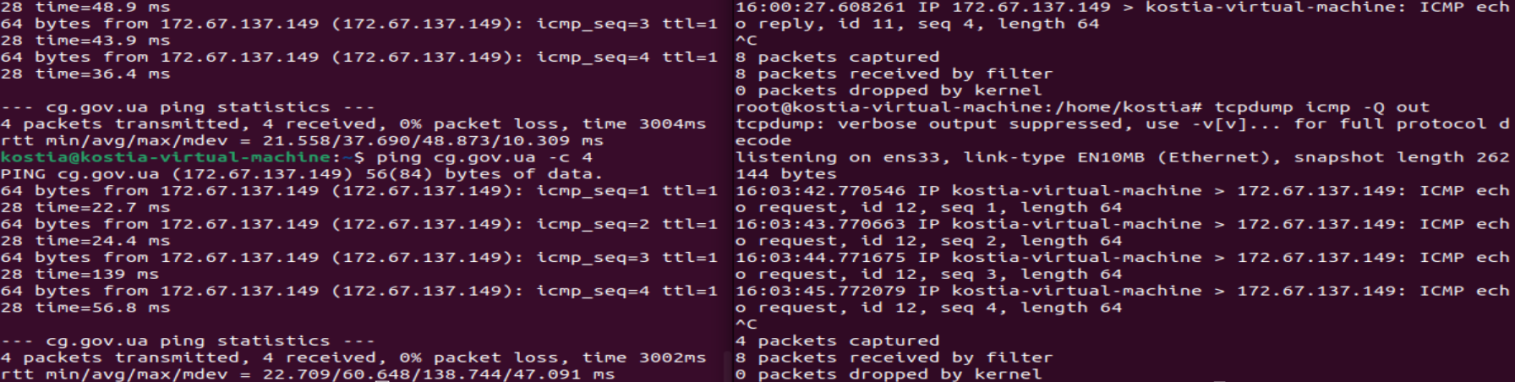
1. Обрана адреса – **sm**.**gov.ua,**

її IP-адреса – 172.67.137.149 або 104.21.64.232 (під час пінгування адреса змінилася на 3 хв)

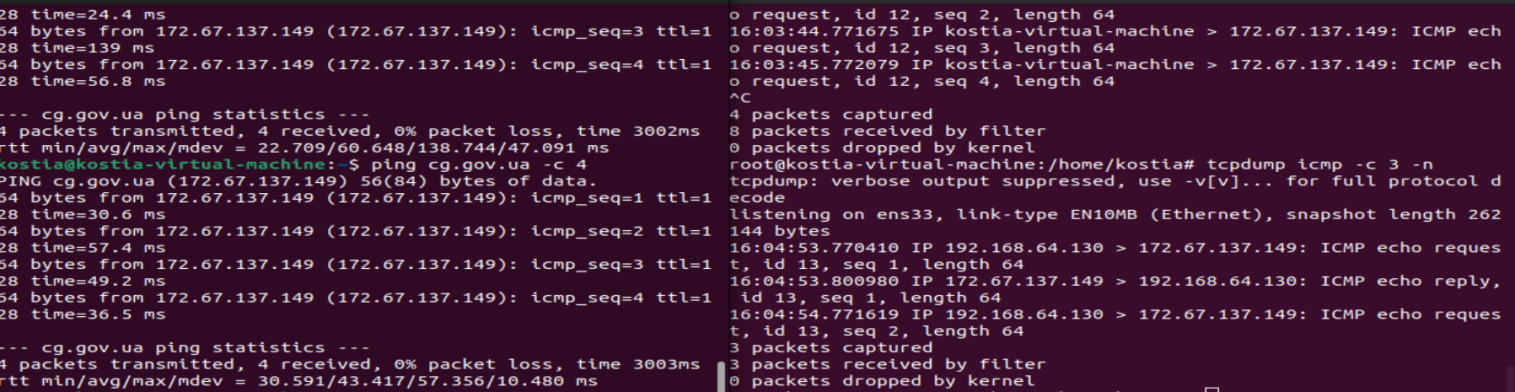
1. Застосування фільтру для перехоплення **всіх icmp пакетів** створених **чотирма** ехо-запитами до обраного сайту.



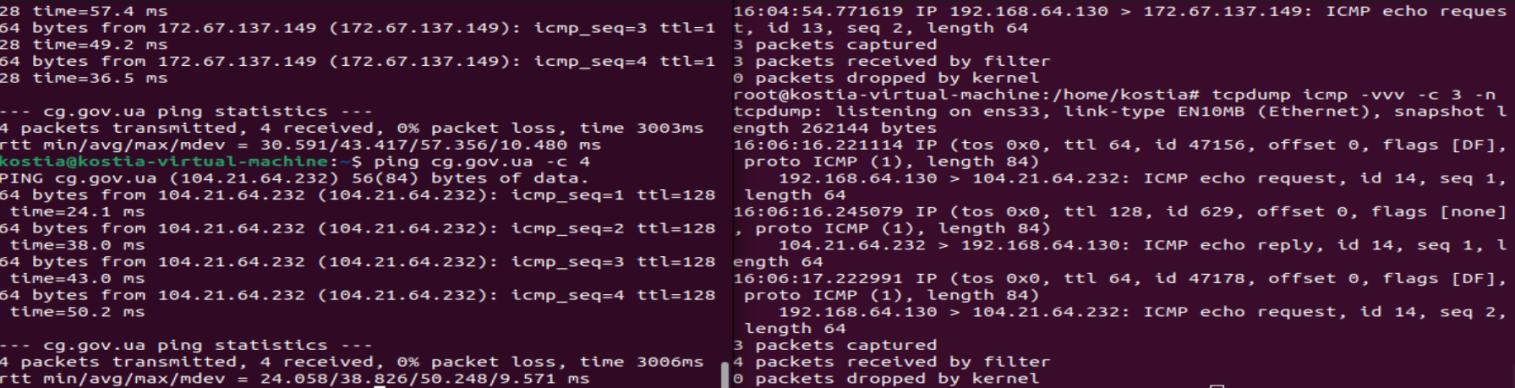
1. Застосування фільтру для перехоплення **icmp відповідей** створених **п’ятьма** запитами до обраного сайту.



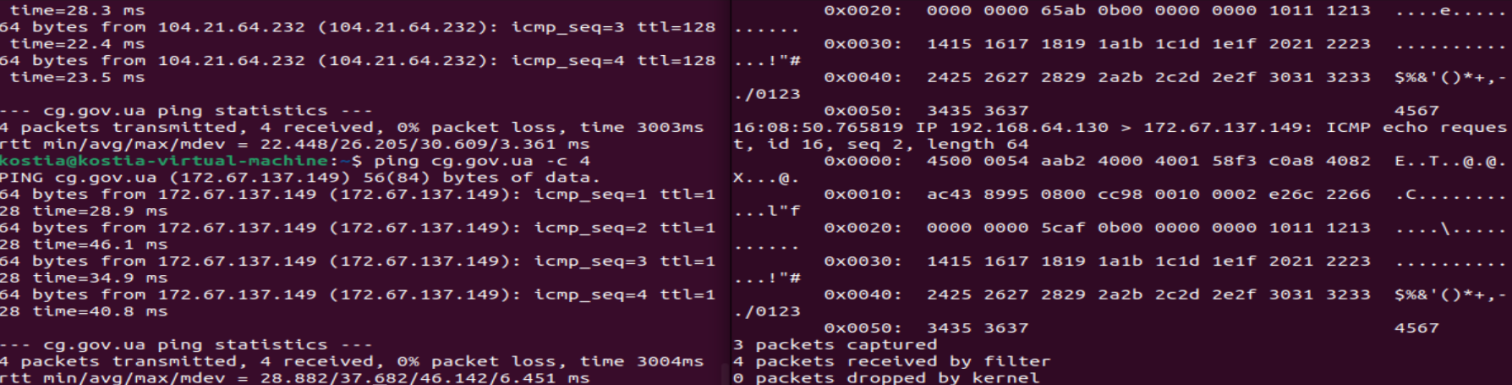
1. Застосування фільтру для перехоплення **лише перших трьох** **icmp відповідей без DNS перетворення** від обраного сайту.



1. Застосування фільтру для максимально деталізованого виводу перехоплених **перших трьох** **icmp запитів** до обраного сайту.



1. Застосування фільтру для виводу payload **в HEX форматі** перехоплених **перших трьох** **icmp запитів**. Зробіть скріншот обох вікон з відображенням даної інформації та скопіюйте у Звіт за дане ПЗ.



tcpdump: verbose output suppressed, use -v[v]... for full protocol decode

listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes

16:08:49.764822 IP 192.168.64.130 > 172.67.137.149: ICMP echo request, id 16, seq 1, length 64

0x0000: 4500 0054 aa84 4000 4001 5921 c0a8 4082 E..T..@.@.Y!..@.

0x0010: ac43 8995 0800 c49d 0010 0001 e16c 2266 .C...........l"f

0x0020: 0000 0000 65ab 0b00 0000 0000 1011 1213 ....e...........

0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .............!"#

0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()\*+,-./0123

0x0050: 3435 3637 4567

16:08:49.793655 IP 172.67.137.149 > 192.168.64.130: ICMP echo reply, id 16, seq 1, length 64

0x0000: 4500 0054 0298 0000 8001 010e ac43 8995 E..T.........C..

0x0010: c0a8 4082 0000 cc9d 0010 0001 e16c 2266 ..@..........l"f

0x0020: 0000 0000 65ab 0b00 0000 0000 1011 1213 ....e...........

0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .............!"#

0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()\*+,-./0123

0x0050: 3435 3637 4567

16:08:50.765819 IP 192.168.64.130 > 172.67.137.149: ICMP echo request, id 16, seq 2, length 64

0x0000: 4500 0054 aab2 4000 4001 58f3 c0a8 4082 E..T..@.@.X...@.

0x0010: ac43 8995 0800 cc98 0010 0002 e26c 2266 .C...........l"f

0x0020: 0000 0000 5caf 0b00 0000 0000 1011 1213 ....\...........

0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223 .............!"#

0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()\*+,-./0123

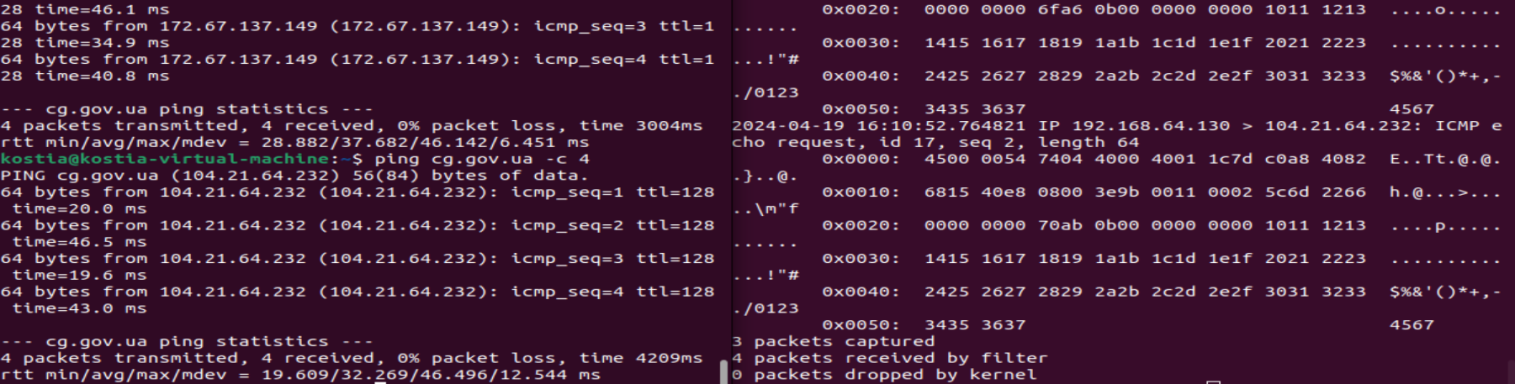
0x0050: 3435 3637 4567

3 packets captured

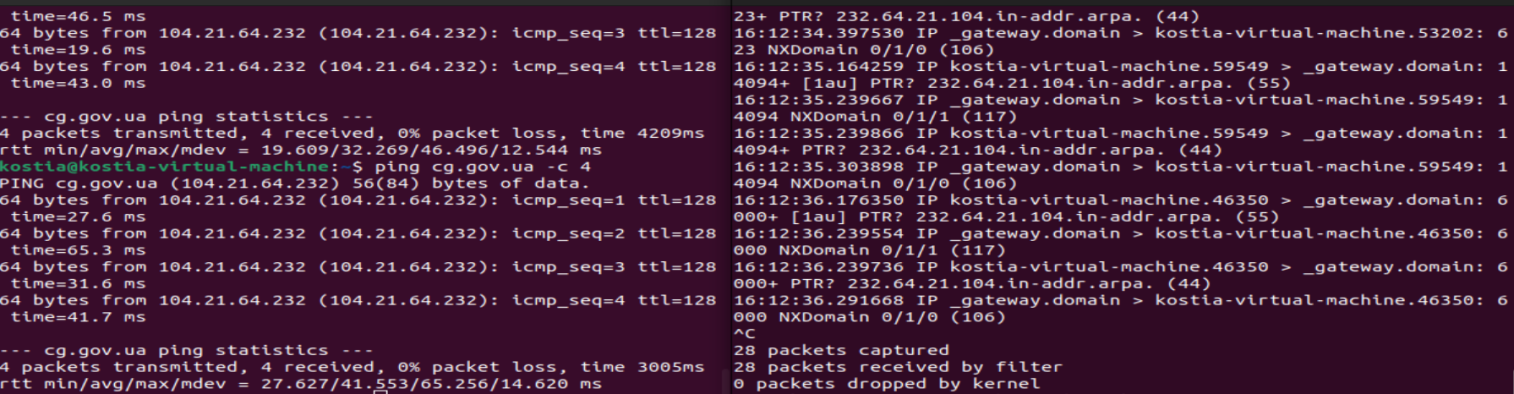
4 packets received by filter

0 packets dropped by kernel

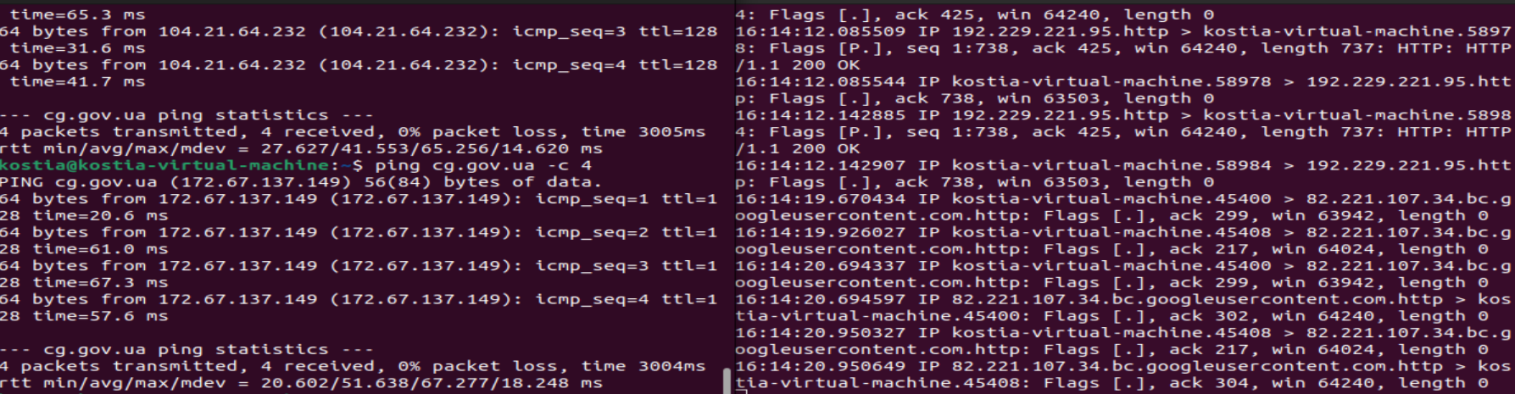
1. Для попереднього пункту змінено **формат часу** для виводу перехопленого трафіку, який починає відлік від першого перехопленого пакету.



1. Застосування фільтру для **перехоплення DNS трафіку** для визначення IP адреси обраного сайту.



1. Застосування фільтру для **перехоплення http** **трафіку**
2. Результат застосування модифікованого фільтру з метою **відбору пакетів лише обраного сайту**.



**Висновок:** утиліта tcpdump дозволила відстежити мережевий трафік, пов'язаний з зверненням до веб-сайту sm.gov.ua. Шляхом аналізу отриманих пакетів було встановлено IP-адресу сервера, з якого надходили відповіді на запити до sm.gov.ua та час відповіді. Такий підхід до моніторингу мережевого трафіку є корисним для виявлення можливих проблем з доступністю веб-сайту або швидкістю його завантаження.

Отже, використання утиліти tcpdump дозволило здійснити докладний аналіз мережевого трафіку, пов'язаного з веб-сайтом сп.gov.ua шляхом його пінгування і захоплення трафіку з практичним відпрацюванням функціоналу утиліти у різних режимах.