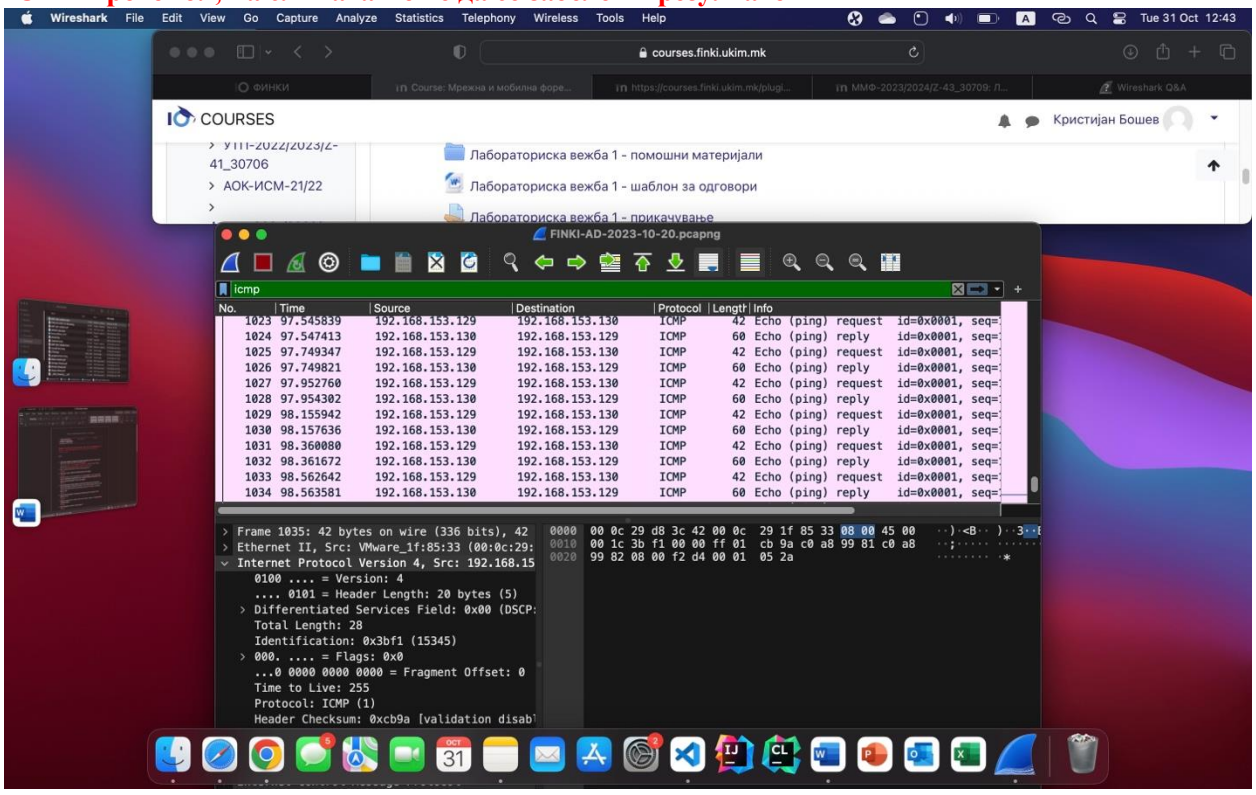
Лабораториска вежба 2 – Откривање на ексфилтрација на податоци и IPFIX анализа	*Име и презиме* *Кристијан Бошев*	*Индекс* *203159*

Напомена: Сите одговори треба да бидат напишани со црвена боја. На секој screenshot што ќе го поставите во елаборатот, осигурајте се дека се гледа вашето најавено име на Courses и моменталното време.

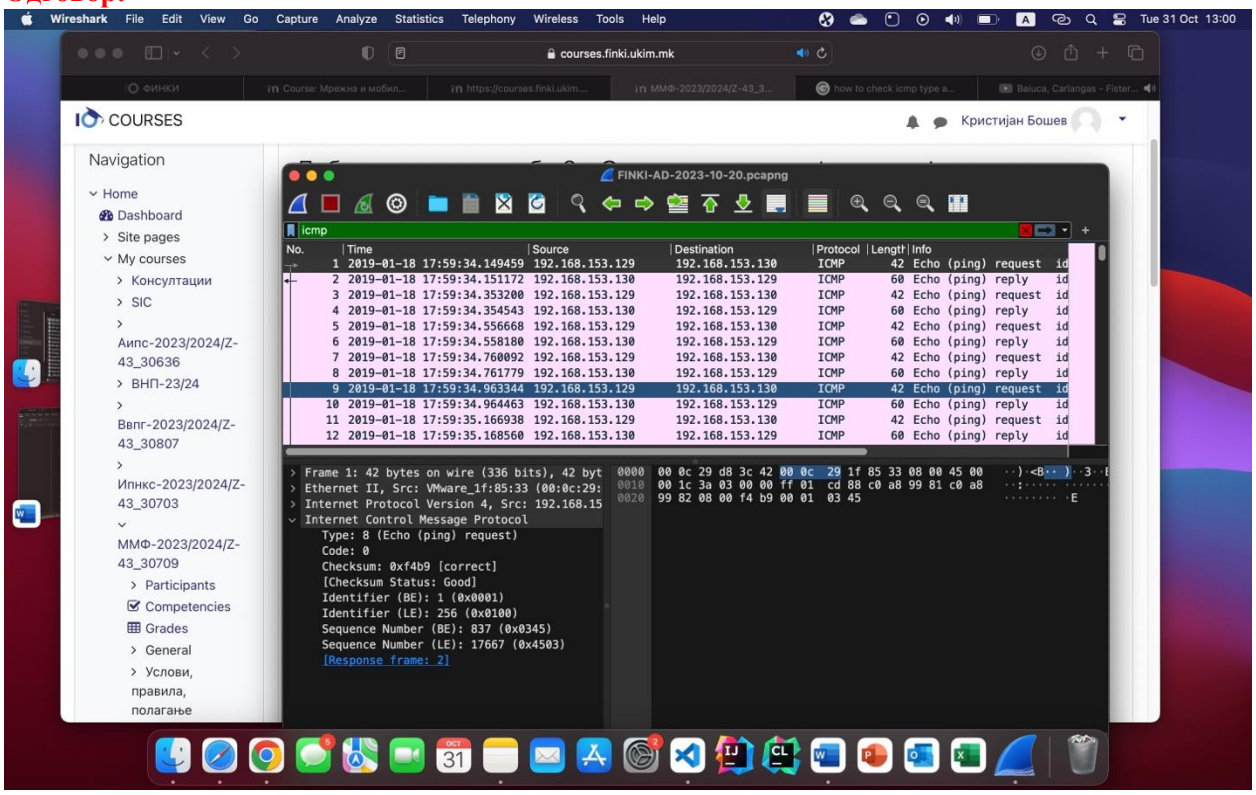
Дел 1

1. Помеѓу кои дестинации се испраќаат echo request и echo response пакетите? Колку вкупно пакети имаат размената меѓу себе овие две дестинации?
   Одговор: Echo request i response porakite se isprakjaat pomegju Src: 192.168.153.129, Dst: 192.168.153.130 adresite, vkupno pomegju niv ima 1018 paketi razmeneto
2. Како ја изведовте оваа активност? Поставете слика од резултатот.
   Одговор:Оваа активност ја спроведив така што, ги филтрирав сите пакети кој имаат ICMP протокол, на сликата може да се забележи резултатот



3. Од кој `type` и `code` се разменетите ICMP барања? Кој кого пинг-а?

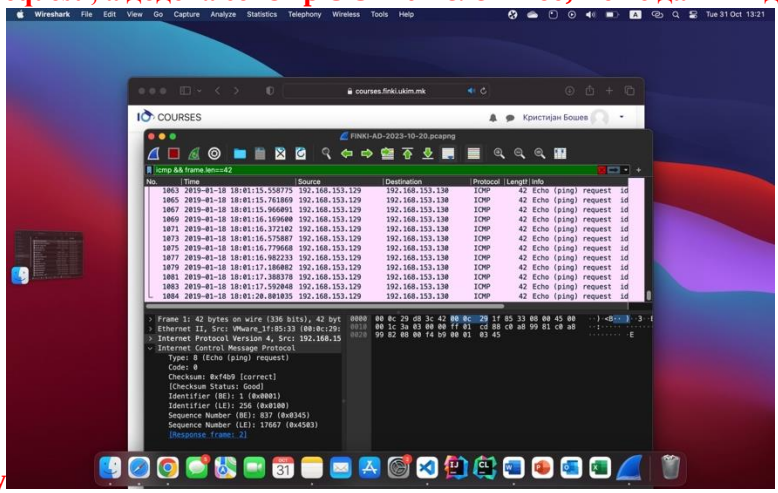
Одговор:



Како што можи да видиме на сликата echo ping request спаѓа под Type 8, и code 0
А додека, на ист начин видов за echo ping reply спаша под type 0 и code 0. Ping командата испраќа ICMP Echo request до некој хост или рутер и потоа очекува одговор од него.

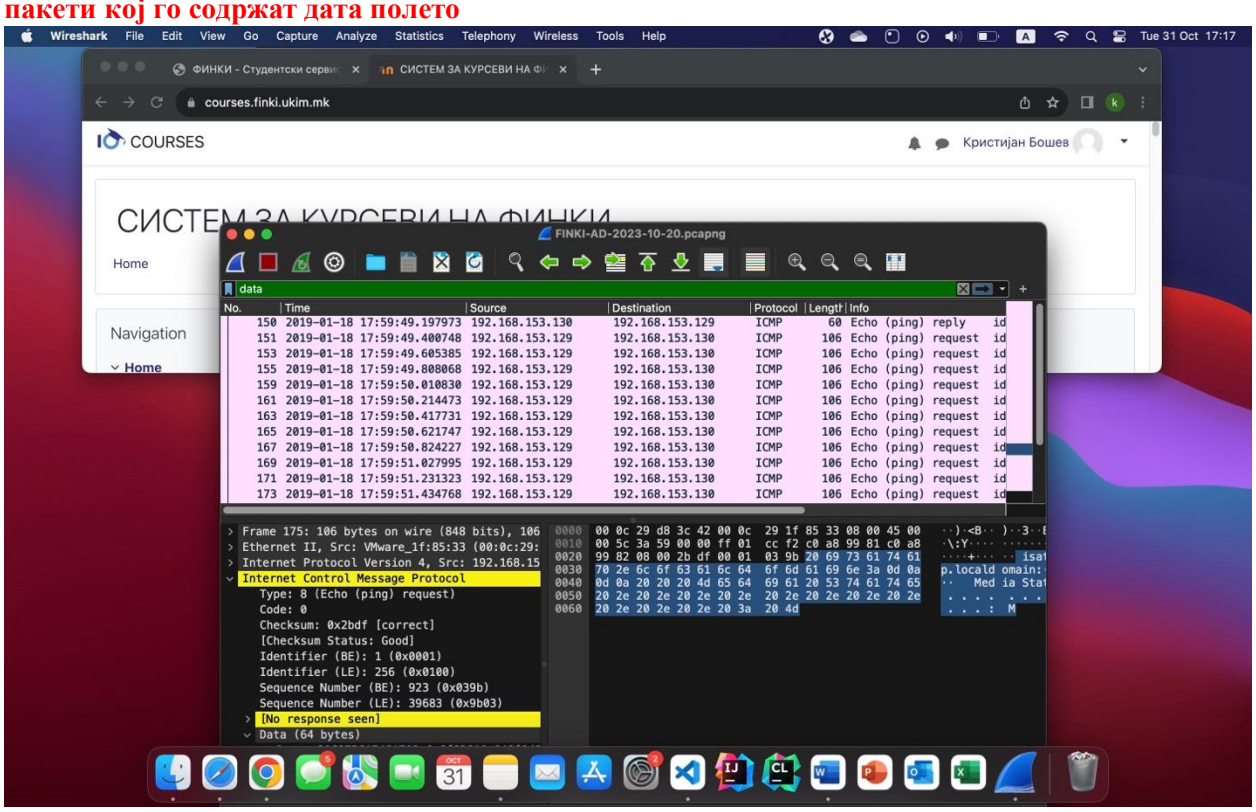
4. Напишете филтри со кои ќе се прикажат исклучиво `echo request`, а потоа и `echo response` пакетите. Користената синтакса вклучете ја во одговорот во шаблонот. Колку вкупно `echo request` пакети биле испратени? А колку `echo response`?

Одговор:Преку овај филтер icmp && frame.len==42 можеме да ги излистаме сите пакети кој што се request , а додека со icmp && frame.len==60, може да ги видиме сите пакети кој што се reply



Преку вметнување на соодветниот филтер и *Statistics -> Capture File Properties* можеме да видеме колку паќете се филтрирани.Echo.request = 495, Echo reply 508

5. Пред да продолжите понатаму, пробајте да дадете претпоставка зошто две станици би се разменале волкав број на ping пораки. Истражете за некои познати напади со помош на ICMP и дадете кратко објаснување (една-две реченици) за секој од нив. Потребно е да објасните барем 2 напада.
   Одговор:Бидејќи станува збор за напад и можеби напаѓачот сакал да го успори крајниот систем, еден од познатите напади е Ping of Death (*Пинг на смртта*) или познат уште и како Ping Flood е олд-скул тип на DDoS напад кој манипулира со IP протоколи со цел испраќање малициозни пингови до системот. Практично, со испраќање на неконвенционални ping-пакети чија големина значително ја надминува максималната дозволена вредност од 65,535 бајти, Друг напад е Smurf нападот го менува изворот на праќање на echo request пакети.
6. Дали успеавте да забележите отстапување во големината кај некои од пакетите? Која е причината за тоа?
   Одговор:Најчесто нивната големина варира поради флексибилноста на payload size,енкапсулацијата на ICMP во IP и LINK layer headers.
7. Водејќи се според она што се наоѓа во `data` делот на пакетите, пробајте да го реконструирате и објасните нападот.
   Одговор:Цело време се преплавува крајниот систем со ping
8. Која е IP адресата на напаѓачот, а која на жртвата?
   Одговор:Адреса на напаѓачот е 192.168.153.129 а додека на жтрвата е 192.168.153.130
9. Напишете филтер со кој ќе ги излистате исклучиво оние ICMP пораки кои содржат `data` дел
   Одговор:Потребниот филтер е “data” преку овај филтер можеме да ги излистаме сите пакети кој го содржат дата полето



10. Што добивте на излез? Најдете начин како ова да го претворите во ASCII репрезентацијата и објаснете ја декодираната содржина.
    Одговор Огромен број на броеви кој што се во хексадецимален формат, корисникот

пробва да се поврзе на мрежа, но повеќе пати е спречен со пораката, media state……media disconected

11. Кратко опишете му на СТО-то за каков тип на напад станува збор и како бил изведен. Се разбира, описот внесете го во елаборатот.
    Одговор:Станува збор за DoS attack каде корисникот е спречен да се поврзе на мрежата преку некаков малициозен софтвер.
12. Истражете дали постојат бесплатни алатки кои би ви овозможиле да направите ваков напад на дадена мрежа. Поставете линкови.
    Одговор:HOIC- https://www.imperva.com/learn/ddos/high-orbit-ion-cannon/
    HULK DDos Script- https://github.com/R3DHULK/HULK
    Thor's hammer - https://sourceforge.net/projects/torshammer/
    Овие се едни од попознатите алатки за вршење на DoS напади

Дел 2

13.Пробајте да ја испечатите на екран содржината од добиената `.yaf` датотека. Што гледате?
Одговор: Може да се увиди дека станува збор за различен формат во однос на нашата зачувана .pcap датотека.

14. Споредете ја големината на оригиналната `.pcap` датотека и добиената `.yaf` датотека. Дали постои разлика во големината? Зошто?
Одговор:Големината на .pcap датотеката е значително пголема во однос на .yaf датотеката, затоа што се чува податоци за секој пакет поединечно, а додека во .yaf датотеката можеме да видеме дека се чува flow data.

15..Поставете ги првите 10 линии од генерираната текстуална датотека во елаборатот.
ВНИМАНИЕ: Не ја поставувајте целата содржина
Одговор:

```
FlowRecord 1:
  Source IP: 192.168.64.1
  Destination IP: 192.168.64.4
  Source Port: 53
  Destination Port: 36269
  Protocol: DNS
  Bytes Transferred: 108
  Packets: 10
  Start Time: 2023-11-05 10:03:31
    End Time: 2023-11-05 10:05:07
```

16.Колку записи се наоѓаат во SiLK датотеката? Дали се користи компресија?
Одговор:Има голем број на записи, SILK е направен за да обработка на огромен број на flow податоци, и притоа тој користи компресија.
17.Која била најчестата дестинациска порта во вашиот сообраќај? Колку пакети биле упатени кон неа?
Одговор:Најчеста дестинациска порта е 40803, биле упатени вкупно 434 пакети.
18.Кој е најчесто контактираниот /24 subnet од вашиот capture file? Пробајте да откриете кому му припаѓа.
Одговор:
19.Напишете сопствена скрипта во јазик по избор или најдете готова алатка која ќе ви овозможи секоја IP адреса да ја парсирате од излезот на `rwuniq` командата, а потоа ќе најде географска локација и hostname. Името на алатката или начинот на којшто сте ја изработиле сопствената скрипта ставете ги во елаборатот (не е потребен изворниот код, само кратката постапка и како сте успеале да ги добиете посакуваните информации). Задолжително поставете слика со кое го демонстрирате работењето на решението. Каде се наоѓа најпосетуваната IP адреса?
Одговор:
20.Со колкав % од сите пакети учествува вашата најпосетувана IP адреса?
Одговор:Најпосетуваната адреса учествува со 36,7% од сите пакети.

21.Обидете се да ја адаптирате претходната команда со тоа што сега приказот да се изврши во однос на дестинациската порта.
Одговор:Најчестата дестинациска порта учествува со околу 7,3% од сите други дест.порти.

22.Поставете слика со излез од претходно извршената команда врз некоја поголема IPFIX датотека која сте ја нашле на Интернет и сте ја конвертирале во SiLK формат.

Одговор Многу тешко се наоѓа IPFIX датотека на интернет.