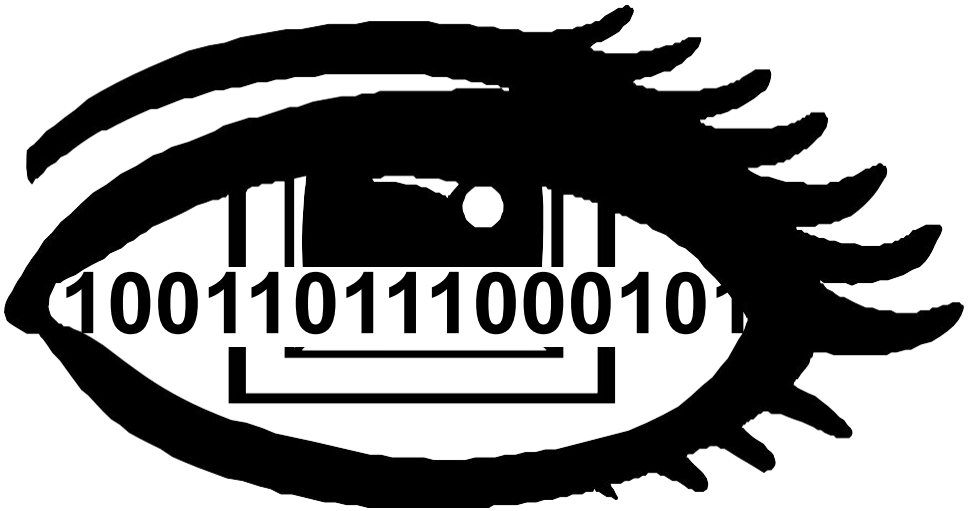
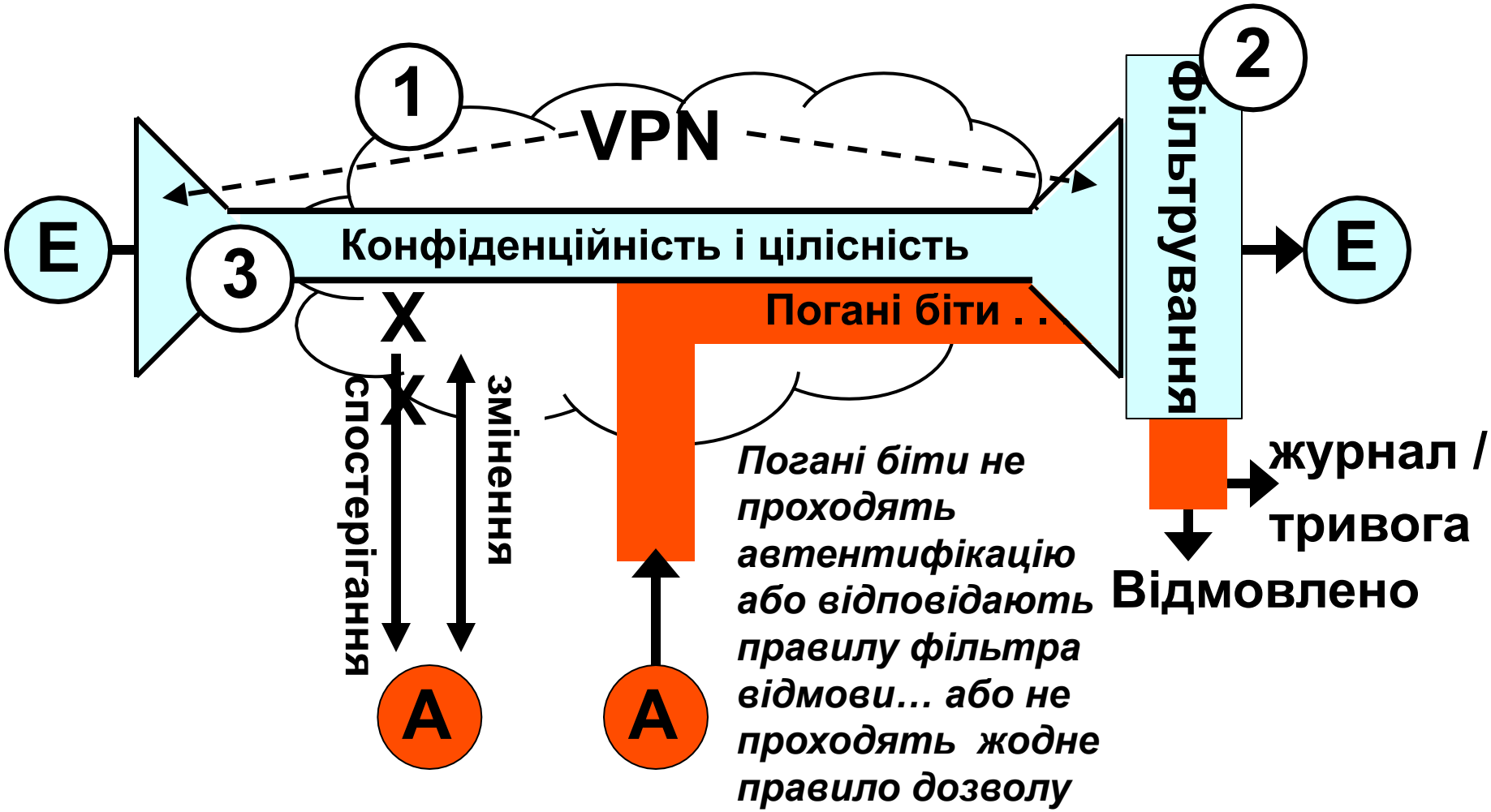
Мережева безпека



Аналіз трафіка
та
сигнатури атак

Модель мережевої безпеки (фільтрування та криптологія)



Перелік тем

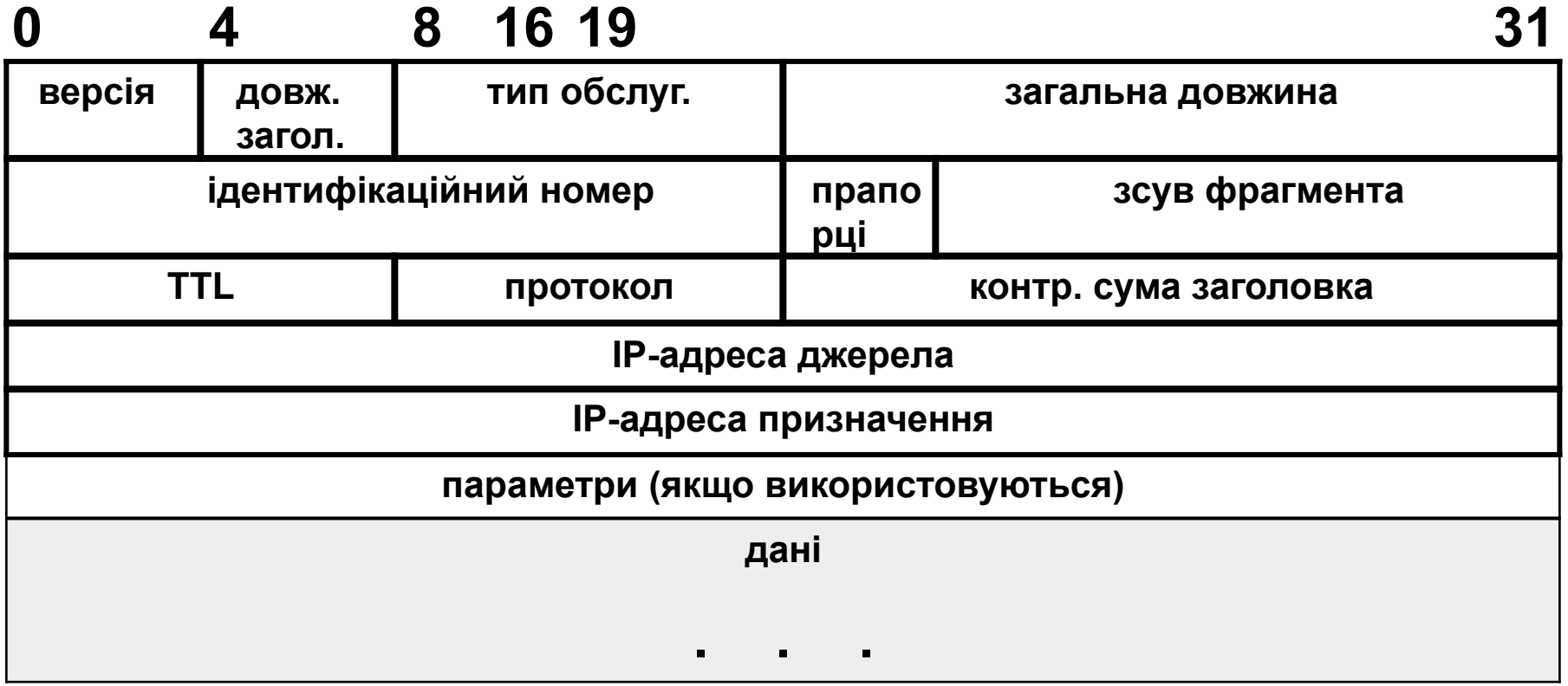
- Читання вихідного шістнадцяткового трафіка.
- Ознайомлення зі зчитуванням «трасувань» пакетів.
- Розпізнавання нормальних/аномальних ситуацій.
- Розгляд деяких «класичних» атак.
- SYN cookies (і механізм MAC).
- Визначення «відбитків» ОС (активне і пасивне).

«Перегляд» мережевого трафіка

- Перегляд вихідного потоку бітів є технічно невиправданим, тому ми будемо використовувати спеціальну програму, що називається аналізатор протоколів, для захоплення, трансляції та представлення пакетів у зручній для людини формі.

- Інтерпретація відповідно до форматів заголовків, визначених у документах RFC, справа нескладна.

Поля заголовка IP



- **Версія: наразі — 4.**
- **Довжина заголовка: к-ість 32-бітних слів у заголовку.**
- **Загальна довжина: к-ість байтів у всьому пакеті; макс. 65 535 ($2^{16} – 1$).**

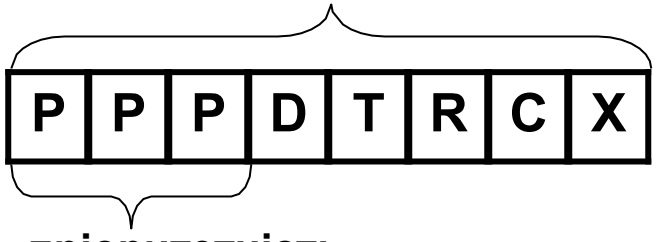
Поля заголовка IP

- **Ідентифікаційний номер: унікальний номер кожного пакета, що слугує для відновлення дейтаграм із фрагментів.**
- **Прапорці: XDM:**
  - **X — зарезервований, завжди 0;**
  - **D = 1 Don’t Fragment («не фрагментувати»);**
  - **M = 1 More Fragments («є ще фрагменти»).**
- **Зсув фрагмента: положення фрагмента у вихідній дейтаграмі (в одиницях по 8 байтів).**
- **TTL — Time To Live («тривалість життя»): верхня межа кількості маршрутизаторів, через які може пройти дейтаграма.**
- **Контрольна сума заголовка: тільки для інформації заголовка IP, інкапсульовані протоколи 4-го рівня зазвичай мають свої контрольні суми.**
- **IP-адреса джерела/призначення: говорить саме за себе.**

Поля заголовка IP

- **Тип обслуговування: (8 бітів) Аналіз трафіка №6**

Старіший формат RFC 791/1349

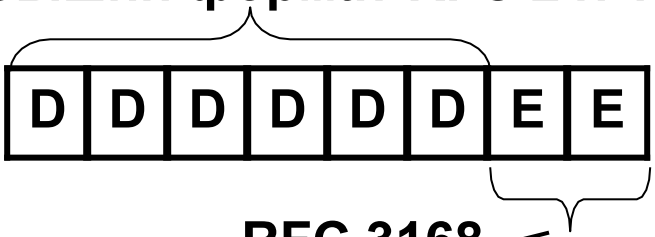


PPP — пріоритетність, ніколи не використовується, див. RFC 1195

додано в RFC 1455

- **D = 1 — мінімізувати затримку;**
- **T = 1 — максимізувати пропускну спроможність;**
- **R = 1 — максимізувати надійність;**
- **C = 1 — мінімізувати вартість;**
- **зазвичай встановлюється тільки 1 біт одночасно;**
- **DTRC = 0000 — нормальне опрацювання;**
- **DTRC = 1111 — максимізувати безпеку;**
- **X — зарезервований, завжди 0.**

Новіший формат RFC 2474



RFC 3168

- **DDDDDD — точка коду диференційованих послуг (Differentiated Services Code Point, DSCP), яка «вказує» на одне з 2^6 визначень служб;**
- **EE — явне повідомлення про перевантаження (Explicit Congestion Notification, ECN) (додано в 2001).**

Поля заголовка IP

- **Номер протоколу: визначає протокол рівня вище, дані якого передаються в IP-пакеті/дейтаграмі.**
- **Деякі найбільш відомі протоколи (із десятковими номерами портів):**
  - **1 ICMP**
  - **6 TCP**
  - **9 IGRP**
  - **17 UDP (0x11)**
  - **47 GRE (0x2F)**
  - **50 ESP (0x32)**
  - **51 AH (0x33)**
  - **88 EIGRP**
  - **89 OSPF**
  - **115 L2TP тощо**

Із повним переліком можна ознайомитися на сайті www.iana.org.

Поля заголовка IP

- **Параметри: список змінної довжини (0–40 байтів із заповненням нулями до 32-бітної межі за потреби) додаткових інструкцій опрацювання пакета, що підтримуються не всім хостами чи маршрутизаторами.**
  - **Якщо параметр задається, для вказання, що це за параметр, використовується один байт.**
  - **Приклади:**
    - **0x07 □ Record Route (записувати маршрут, параметр IP);**
    - **0x44 (68_{10}) □ Timestamp (мітка часу, параметр IP);**
    - **0x89 (137_{10}) □ Strict Source Route (чітка маршрутизація від джерела, параметр IP);**
    - **0x02 □ Maximum Segment Size (максимальний розмір сегмента, параметр TCP).**

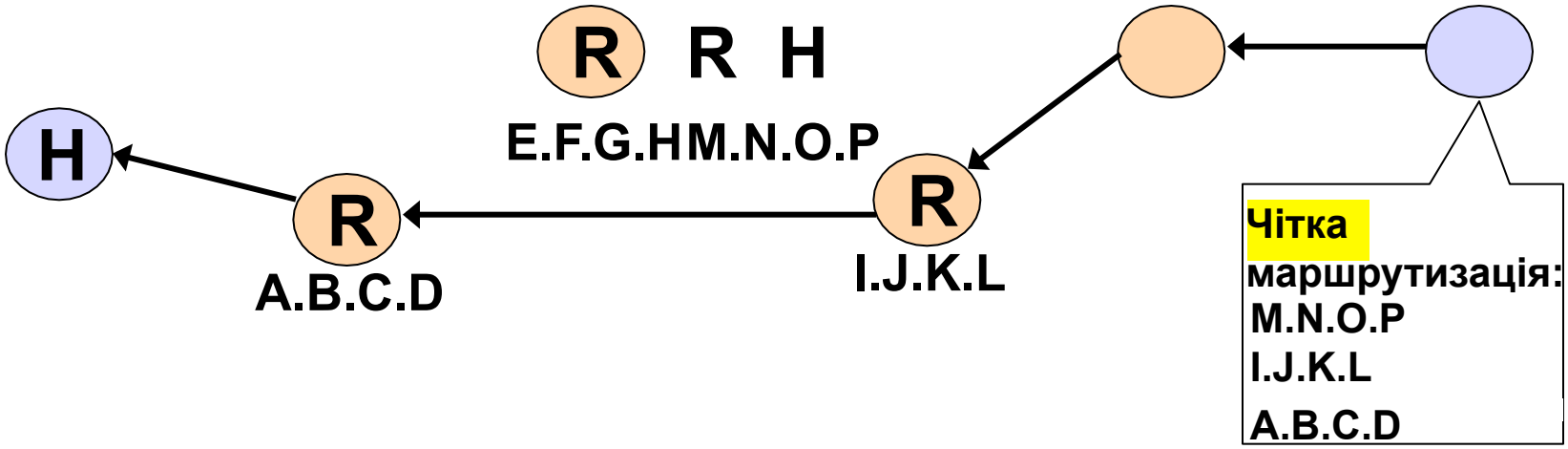
Поля заголовка IP

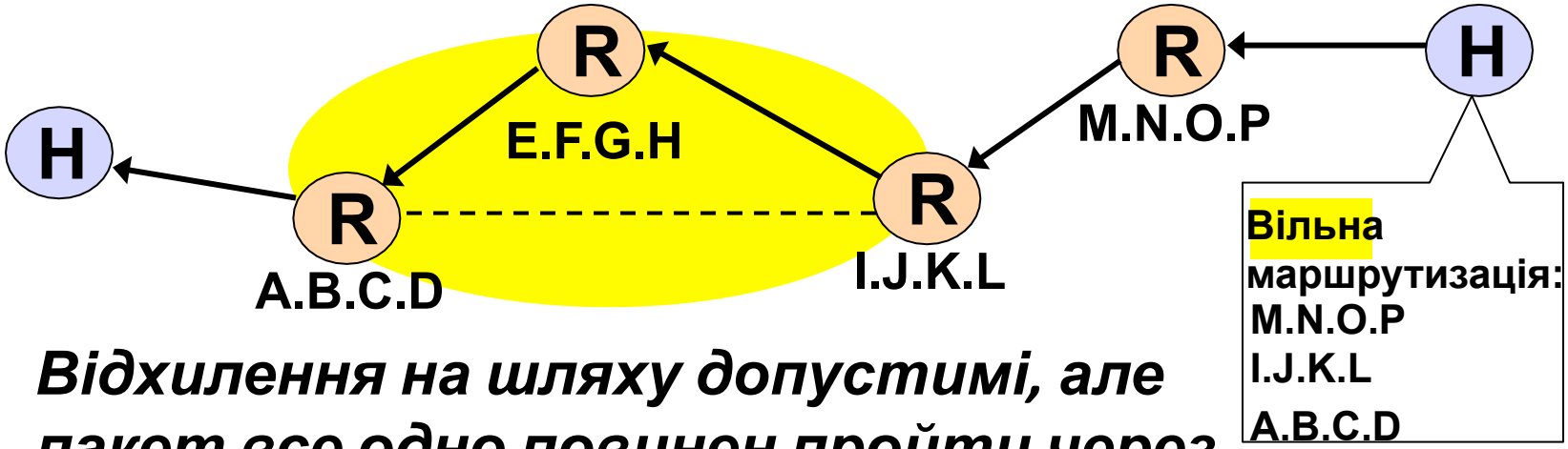
- **Приклади (продовження):**
  - **Record Route (RFC 791): >ping –r задає параметр «записувати маршрут» у вихідній дейтаграмі, і маршрутизатори на шляху її пересилки записують свої вихідні IP-адреси в поле параметрів.**
  - **Source Routing: механізм для визначення відправником маршруту, яким має пройти дейтаграма. Два типи:**
    - **чітка маршрутизація від джерела;**
    - **вільна маршрутизація від джерела.**

IP-маршрутизація від джерела

- **Чітка маршрутизація від джерела: відправник задає точний шлях, і маршрутизатор, який не може дотримати це правило, повертає ICMP-повідомлення «source route failed» («не вдалося дотримати шлях від джерела»).**
- **Вільна маршрутизація від джерела: відправник задає список IP-адрес, через які пакет повинен пройти на своєму шляху, але маршрутизатори на шляху можуть пересилати його на додаткові проміжні IP-адреси.**
- **Формат поля параметрів IP для маршрутизації від джерела:**
  - **код: 0x89 (чітке) або 0x83 (вільне);**
  - **довжина: кількість байтів усього в полі параметрів;**
  - **покажчик: номер за списком IP-адрес, який «указує» на IP-адресу наступного переходу;**
  - **відсутність операцій: 0x01 (для заповнення);**
  - **<перелік до _____ (к-сть) IP-адрес маршрутизаторів>.**

Чітка та вільна маршрутизація від джерела





Відхилення на шляху допустимі, але пакет все одно повинен пройти через кожен маршрутизатор у списку в заданому порядку

Поля заголовка TCP

- Номери портів джерела і призначення: говорять за себе.
- Порядковий номер: число в першому байті інкапсульованого корисного навантаження у межах усього потоку даних від відправника.
- Довжина заголовка: к-ість 32-бітних слів у заголовку TCP.

Поля заголовка TCP

- **Номер підтвердження: наступний порядковий номер, що його відправник очікує отримати від хоста на іншому кінці з'єднання; по суті, цей параметр слугує для підтвердження отримання всіх байтів із номерами менше ніж номер підтвердження.**
- **Зарезервовано: втім, документ RFC 3168 від 2001 року передбачає використання 2 крайніх правих (із 6 загалом) бітів для контролю перенавантаження.**
- **Розмір вікна: кількість байтів, для отримання яких у відправника є простір.**
- **Контрольна сума: охоплює заголовок TCP, частини заголовка IP, а також інкапсульовані дані.**
- **Вказівник важливості: береться до уваги тільки за встановленого прапорця URG, до порядкового номера додається номер для вказання останнього байта даних у корисному навантаженні, позначених як важливі.**

Поля заголовка TCP

•6 прапорців TCP:

– **Важливо (URG): отримувач має опрацювати дані позачергово: наприклад, користувач перериває сеанс telnet чи завантаження файлу за протоколом FTP (Ctrl + C).**

– **Підтвердження (ACK): береться до уваги номер підтвердження, цей прапорець завжди повинен встановлюватися після початкової частини SYN рукостискання під час встановлення з'єднання.**

– **Просування (PSH): вказівка отримувачу спорожнити свій буфер читання (передати дані з нього на прикладний рівень, не чекаючи на його заповнення) якомога скоріше.**

– **Скидання (RST): скидання з'єднання, наприклад,**

- **запит на з'єднання надходить на TCP-порт, який не прослуховує мережу**
- **(примітка: на запити до UDP-портів, що не прослуховують мережу, видається ICMP-повідомлення «порт недоступний»).**

– **Синхронізація (SYN): порядкові номери прапорців синхронізації для ініціювання нового з' єднання.**

– **Завершення (FIN): відправник завершив надсилання даних; обидві сторони мають «коректно» завершити сеанс, обмінявшись прапорцями FIN.**

Поля заголовка UDP

0	16	31
номер порту джерела	номер порту призначення	
Довжина UDP	Контр. сума UDP	
дані (якщо є) . . .		

Поля заголовка ICMP

- **Типове використання ICMP і повідомлення:**
  - **хост недосяжний (таке повідомлення видає маршрутизатор);**
  - **ехо-запит/ехо-відповідь (ping);**
  - **вповільнення джерела («пригальмуй, ти надсилаєш надто швидко»);**
  - **порт недосяжний (версія прапора скидання TCP для UDP);**
  - **заборонено адміністратором (маршрутизатор/міжмережевий екран заблокував запит);**
  - **перенаправлення (наступного разу спрямовуй свій трафік на маршрутизатор X, а не на мене);**
  - **необхідна фрагментація (але встановлений прапорець DF);**
  - **час перевищено (тобто TTL зменшився до нуля);**
  - **час повторного складання (фрагментів) перевищено.**

https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml

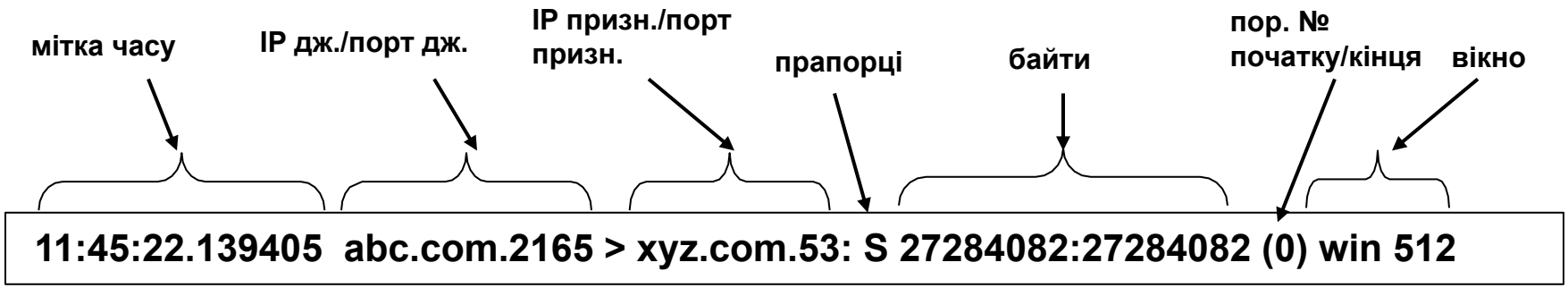
ICMP

- Обмін запитами і повідомленнями керування/про помилки.
- Номерів портів немає, призначення позначається полями типу та коду повідомлення.
- Для обміну даними з хостом службам не потрібно бути активними чи прослуховувати ICMP-трафік, на відміну від TCP і UDP.
- Прослуховують повідомлення ICMP і відповідають на них усі хости!
- ICMP може бути широкомовною розсилкою, TCP — ні.
- В багатьох пристроях (системи виявлення проникнення (IDS), міжмережеві екрани) ехо-відповіді вимикають, щоб вони себе не видавали.
- ICMP-повідомлення про помилки не повинні відправлятися у відповідь на інше ICMP-повідомлення про помилку.

«Перегляд» мережевого трафіка

- Для інтерпретації полів протоколів є багато продуктів:
  - tcpdump і windump (tcpdump.org);
  - sniffer (sniffer.com);
  - etherpeek (wildpackets.com);
  - packet-grabber (wildpackets.com);
  - Wireshark (wireshark.org).
- Приклади пакетів у цьому розділі наводяться у форматах *tcpdump*.
- Інші продукти працюють в аналогічний спосіб.

Аналіз трафіка №1



З чим пов'язаний порт 53? _____

Це UDP- чи TCP-трафік? _____

Що тут відбувається? _____

Примітка: час зазначається із точністю до мільйонної долі секунди за промовчанням.

Примітка: це Syn-пакет, отже корисне навантаження — 0 байтів, на що вказує як те, що порядковий номер кінця збігається з номером початку, так і те, що загальна кількість байтів — 0.

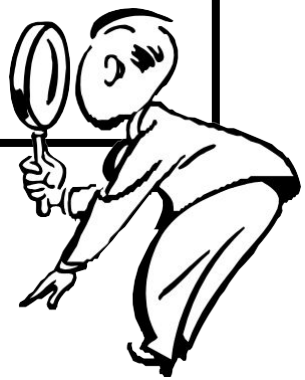
Шістнадцятковий вивід даних

- ***tcpdump*** **не виводить всі поля пакета, якщо не ввімкнути шістнадцятковий вивід.**
- **Приклад: <IP-адреса> [заголовок 4-го рівня] {дані}**

<4500 0028 b5cb 4000 fe01 b229 0102 0304
c0a8 0505> [0000 bc9c bf3c 51ff] {0018 f81b
000d d5f0 000d 63e8 0000 0000 0000}

Інтерпретація заголовка 3-го рівня

<4500 0028 b5cb 4000 fe01 b229 0102 0304
c0a8 0505> [0000 bc9c bf3c 51ff] {0018 f81b
000d d5f0 000d 63e8}



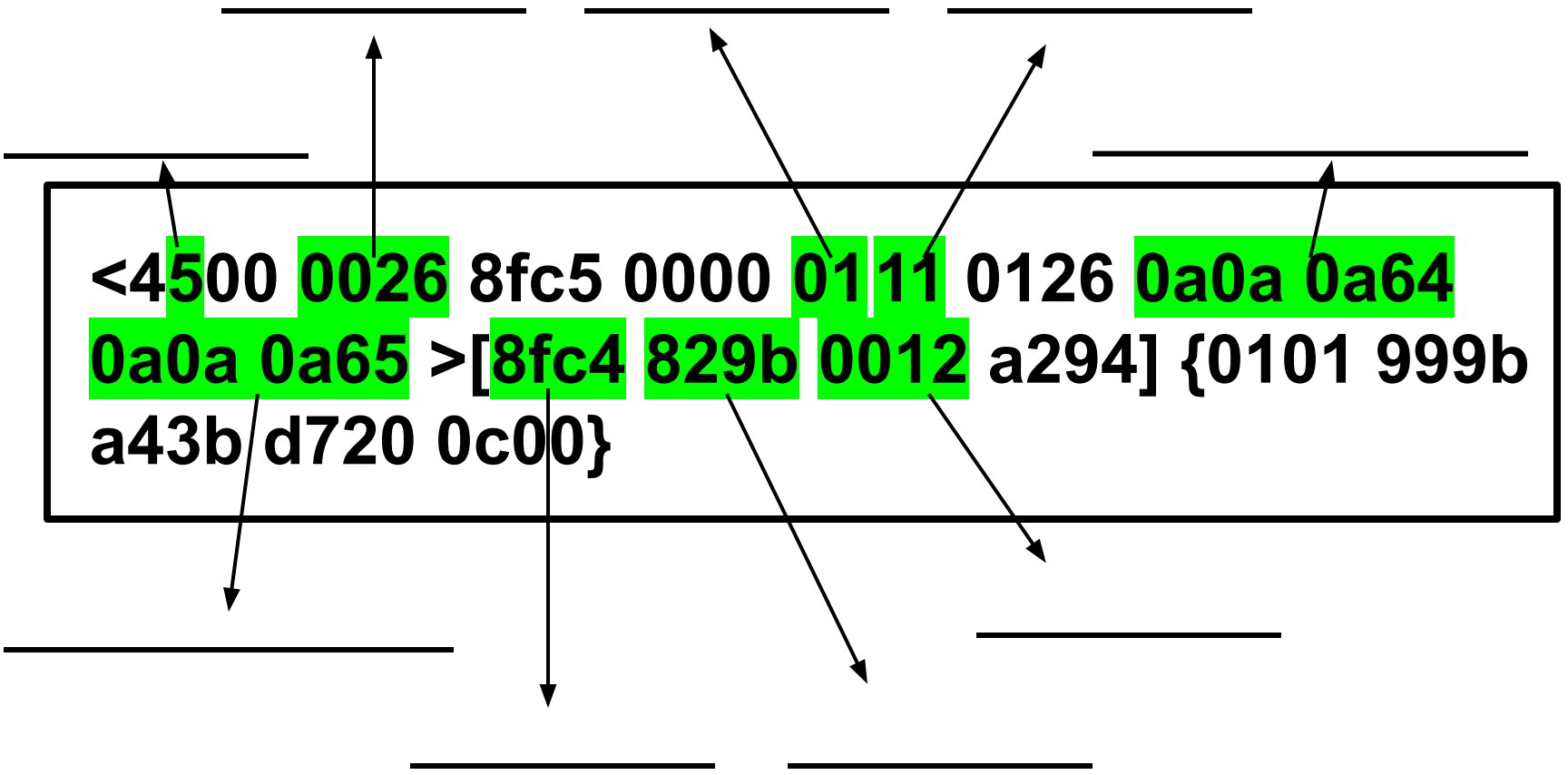
- **Яка довжина заголовка IP (у байтах)? _____**
- **Яка загальна довжина цього пакета? _____**
- **Чи це фрагмент? _____**
- **Яке значення TTL? _____**
- **Який протокол містить у собі цей IP-пакет? _____**
- **Яка IP-адреса призначення в десятковій формі з крапками? _____._____._____._____**

Інтерпретація заголовка 4-го рівня

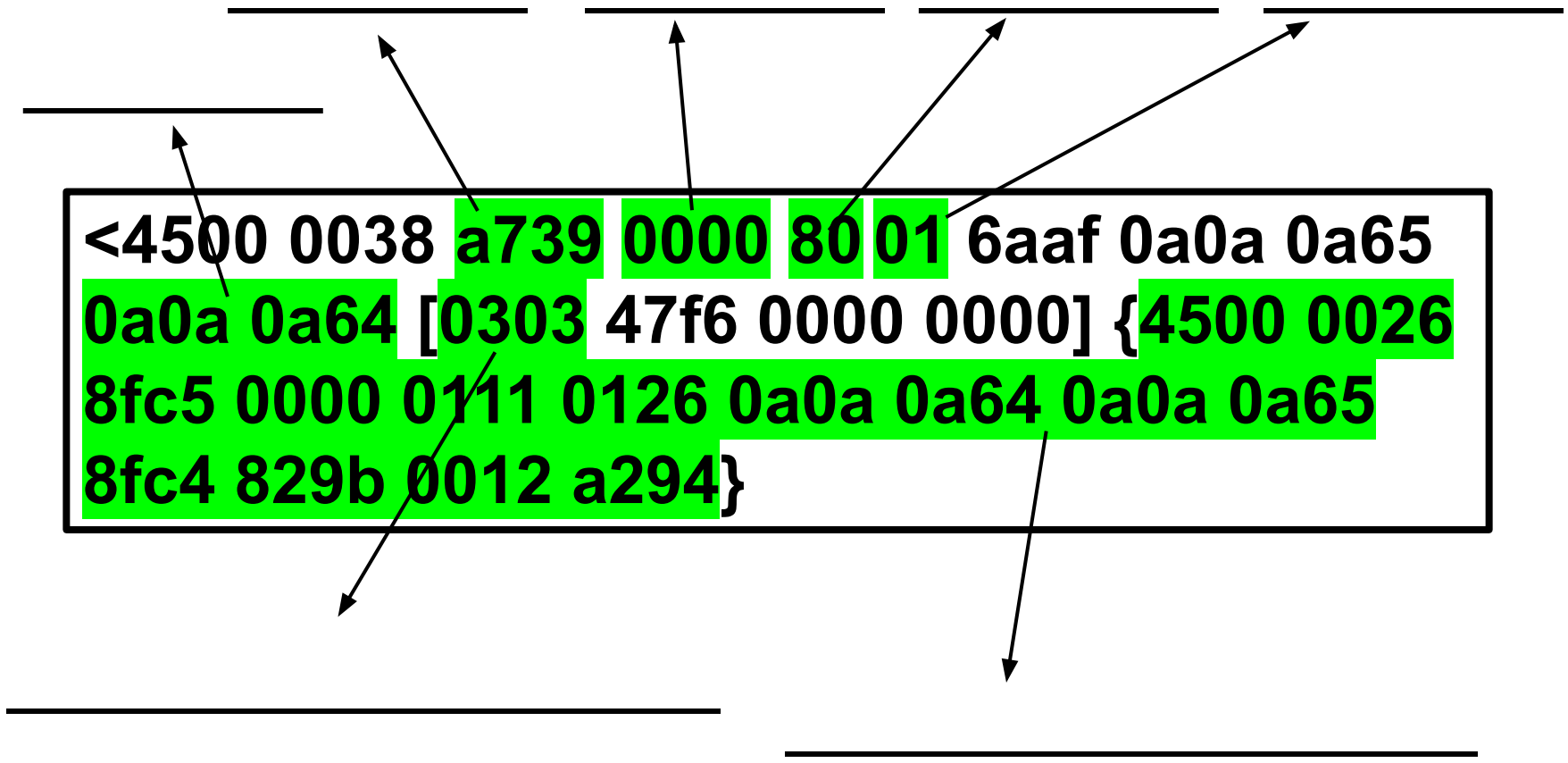
<4500 0028 b5cb 4000 fe01 b229 0102 0304
c0a8 0505> [**0000 bc9c bf3c 51ff**] {0018 f81b
000d d5f0 000d 63e8}

- **Який тип ICMP-повідомлення? _____**
- **Який код ICMP-повідомлення? _____**
- **Що означає bc9c? _____**
- **bf3c (байти 4 і 5) — це ідентифікаційний номер (аналогічно, як в IP-пакеті).**
- **51ff (байти 6 і 7) — це порядковий номер (аналогічно, як в TCP-фрагментах).**

Аналіз трафіка №2



Аналіз трафіка №3



З інструментами простіше!

- Цікаво ж було, чи не так?
- На щастя, здебільшого цю трансляцію виконують інструменти.
- Ось що видав би для попереднього слайда tcpdump:

```
10.10.10.101 > 10.10.10.100: icmp:
10.10.10.101 udp port 33435 unreachable
```

Чудово, лише найважливіше

Аналіз трафіка №4

Екзаменаційні питання

Q1. The packet at right appears to be…

a. going to a Web server.
b. going to a Web client.
c. going to a mail server.
d. going to a mail client.

```
<4600 0034 b245 2000 8c06 b229 d930 6f05
 8378 1228 4400 0000> [0019 d351 3408 7134
 c88a 560a 5002 e27c 0000 0018] f81b 00d1
 c5e0 000d 63e8 0000 0000 0000}
```

Q2. The packet at right has…

a. no IP or TCP options.
b. one or more IP options, but no TCP options.
c. no IP options, but one or more TCP options.
d. one or more IP options and one or more TCP options.

Q3. The packet above is…

a. not fragmented
b. the first fragment (of a fragmented packet)
c. a middle fragment (of a fragmented packet)
d. the last fragment (of a fragmented packet)

Q4. What is the TTL in decimal?

a. 140
b. 6
c. 128
d. 244

Q5. What option is included?

a. Record route
b. Window scale
c. Strict source router
d. Timestamp

Аналіз трафіка №5

13:34:18.330571 vulcan.net.39923 > poseidon.com.25: S 237706227: 237706227 (0) win 8760 <mss 1460> (DF)

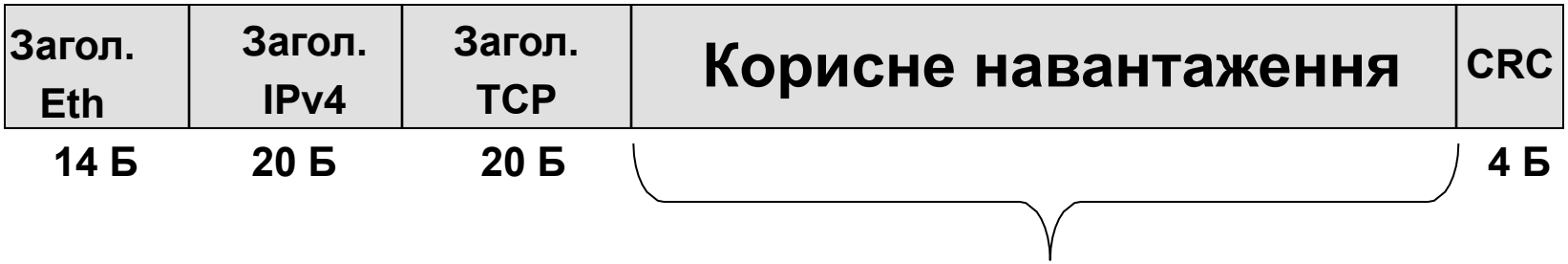
13:34:18.349203 poseidon.com.25 > vulcan.net.39923: S 1430687730: 1430687730 (0) ack 237706228 win 8760 <mss 1460> (DF)

13:34:18.410071 vulcan.net.39923 > poseidon.com.25: . ack 1 win 8760 (DF)

- Що тут відбувається?
- Що означає «mss»?
- Звідки береться 1460?
- Що означає «DF»?
- Чому номер ACK тут скинувся в 1?

MTU і MSS

MTU = 1518



MSS = _____

Аналіз трафіка №6

1. 10.10.10.100.ftp > 10.10.10.33.1054: P 1:81 (80) ack 1 win 32120
2. 10.10.10.33.1054 > 10.10.10.100.ftp: . ack 81 win 8680 (DF)
3. 10.10.10.100.ftp > 10.10.10.33.1054: P 81:117 (36) ack 1 win 32120 (DF) [tos 0x10] Поля заголовка IP
4. 10.10.10.100.ftp > 10.10.10.33.1054: P 117:145 (28) ack 1 win 32120 (DF) [tos 0x10]
5. 10.10.10.33.1054 > 10.10.10.100.ftp: . ack 81 win 8680 (DF)
6. 10.10.10.100.ftp > 10.10.10.33.1054: P 145:174 (29) ack 1 win 32120 (DF) [tos 0x10]
7. 10.10.10.33.1054 > 10.10.10.100.ftp: . ack 81 win 8680 (DF)
8. 10.10.10.100.ftp > 10.10.10.33.1054: P 81:117 (36) ack 1 win 32120 (DF) [tos 0x10]

Запитання щодо аналізу трафіка №6

З1. Яка машина — сервер?

В1. 10.10.10. _____

З2. Чи є в цьому трасуванні 3-етапне рукостискання TCP?

В2. _____(так чи ні)

З3. Який сегмент (корисного навантаження) було втрачено під час передавання від сервера до клієнта?

В3. Сегмент із порядковим номером _____.

З4. Якщо до клієнта надходить пакет №8, яке підтвердження він має надіслати назад на сервер?

В4. ACK № _____.

LaBrea Tar Pit

- Оригінальний інструмент протидії скануванню, розроблений Томом Лістоном.
- Вихідний код доступний за адресою: www.hackbusters.net.
- Причина для такої назви інструмента незабаром стане очевидною.
- Концепція аналогічна ідеї відбивачів і теплових пасток (принад) у захисті проти ракет.
- Зловмисник витрачає процесорні цикли/час на «привид» (тобто хибну ціль).

LaBrea Tar Pit

- **Ось у чому основна хитрість:**
  - **зловмисник надсилає пакети для сканування/промацування IP-адреси, якої не існує;**
  - **локальний маршрутизатор розсилає ARP-запити на цю IP-адресу, якої не існує;**
  - **почувши широмовний ARP-запит, LaBrea запускає таймер; не дочекавшись відповіді за 3 с, LaBrea відповідає: «О, це ж напевне до МЕНЕ, моя MAC-адреса така-то, надсилай цей IP-трафік мені»;**
  - **LaBrea відповідатиме «SYN-ACK» на весь трафік, що надходить, але не відповідатиме на жоден подальший ACK-пакет з цієї конкретної IP-адреси;**
  - **зловмисник продовжує повторювати відправку, чекати на таймаут, повторювати і т. д., поки не відмовиться від марної справи.**

Аналіз трафіка №7 (ще LaBrea)

attacker.com.2045 > victim.org.www S win 8192 (пор. №№ не показані)
victim.org.www > attacker.com.2045 S ack win 10 (пор. №№ не показані)
attacker.com.2045 > victim.org.www ack win 8192 (пор. №№ не показані)
attacker.com.2045 > victim.org.www 1:11 (10) ack 1 win 8192
victim.org.www > attacker.com.2045 ack 11 win 0
attacker.com.2045 > victim.org.www 11:12 (1) ack 1 win 8192
victim.org.www > attacker.com.2045 ack 12 win 0
attacker.com.2045 > victim.org.www 11:12 (1) ack 1 win 8192
victim.org.www > attacker.com.2045 ack 12 win 0
attacker.com.2045 > victim.org.www 11:12 (1) ack 1 win 8192
victim.org.www > attacker.com.2045 ack 12 win 0

. . . це може продовжуватися дуже довго . . .

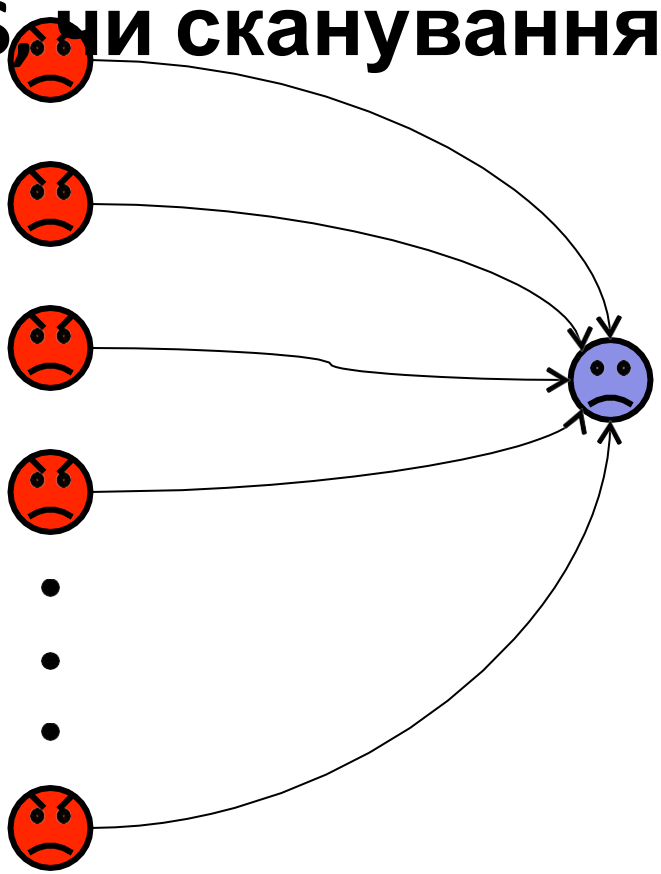
Аналіз трафіка №8

```
14:18:22.5660 bky.net.6041 > svr.login: S 1393892: 1393892 (0) win 4096
14:18:22.5941 svr.login > bky.net.6041 : S 17564:17564 (0) win 54 ack 1393893
14:18:22.6093 bky.net.6042 > svr.login: S 1393893: 1393893 (0) win 4096
14:18:22.6470 bky.net.6043 > svr.login: S 1393894: 1393894 (0) win 4096
14:18:22.6491 svr.login > bky.net.6042 : S 80932:80932 (0) win 54 ack 1393894
14:18:22.7014 bky.net.6044 > svr.login: S 1393895: 1393895 (0) win 4096
14:18:22.7098 svr.login > bky.net.6043 : S 40723:40723 (0) win 54 ack 1393895
14:18:22.7322 bky.net.6045 > svr.login: S 1393896: 1393896 (0) win 4096
14:18:23.0028 bky.net.6046 > svr.login: S 1393897: 1393897 (0) win 4096
. . .
```

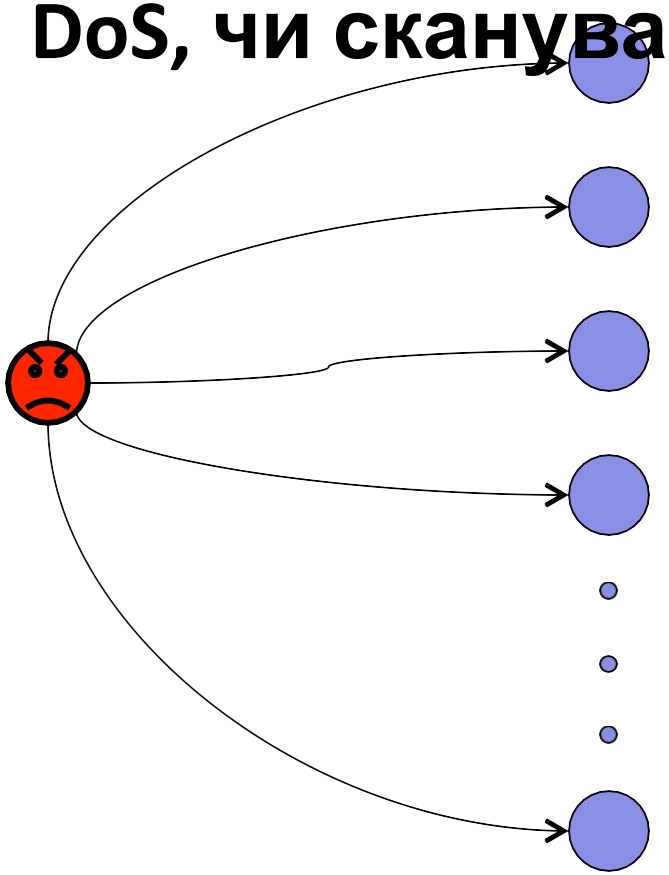
- Що відбувається? _____
- Які наміри в зловмисника? _____
- Чи спрацювало б це, якби номери портів джерела не змінювалися? ____

Узагальнення схем

Чи це більше нагадує DoS, чи сканування?



Чи це більше нагадує DoS, чи сканування?



Боротьба із DoS

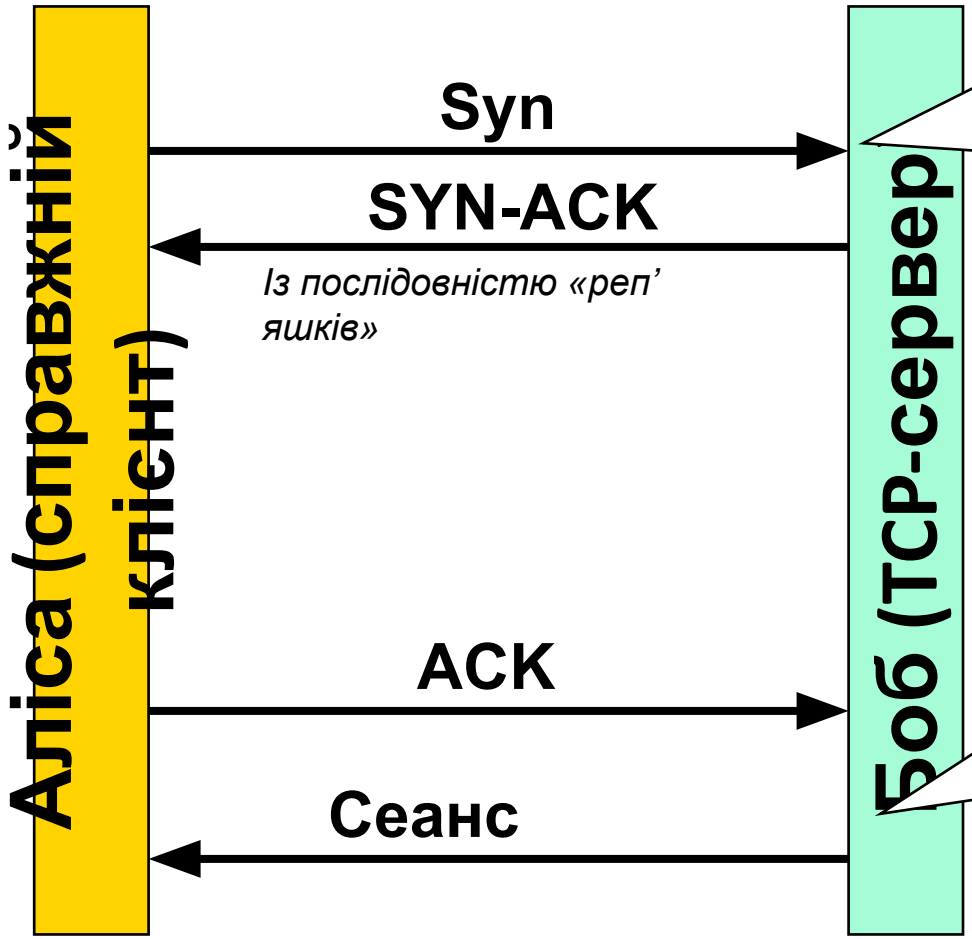
- З RFC 3552 «Настанови з написання текстів документів RFC щодо безпекових міркувань»:
  - (розд. 4.6.3) є два підходи до того, як ускладнити здійснення DoS-атак;
  - (розд. 4.6.3.1) змусьте зловмисника робити більше _____ _____, ніж ви самі;
  - (розд. 4.6.3.2) змусьте зловмисника довести, що він може _____;
  - зміст розд. 4.6.3.2 наведений на наступному слайді.

RFC 3552, розд. 4.6.3.2

Завадити сліпій атаці можливо, змусивши зловмисника довести, що він може отримати дані від жертви. Поширеним методом є примусити зловмисника дати відповідь із використанням інформації, отриманої раніше у результаті обміну повідомленнями. Якщо скористатися цим контрзаходом, зловмисник мусить або використати свою власну адресу (полегшивши своє відстеження), або сфальшувати адресу, яку буде можливо простежити назад уздовж шляху, який проходить через хост, з якого здійснюється атака.

Хости в невеликих підмережах, таким чином, непотрібні зловмиснику (принаймні в контексті атаки з підміною), оскільки атаку можливо відстежити назад до підмережі (чого має бути достатньо для визначення розташування зловмисника), що дасть змогу застосувати заходи захисту від атаки (наприклад, сконфігурувати граничний маршрутизатор відкидати весь трафік з тієї підмережі). Поширеним методом є примусити зловмисника дати відповідь із використанням інформації, отриманої раніше у результаті обміну повідомленнями.

SYN cookies (Реалізація розд. 4.6.3.2)

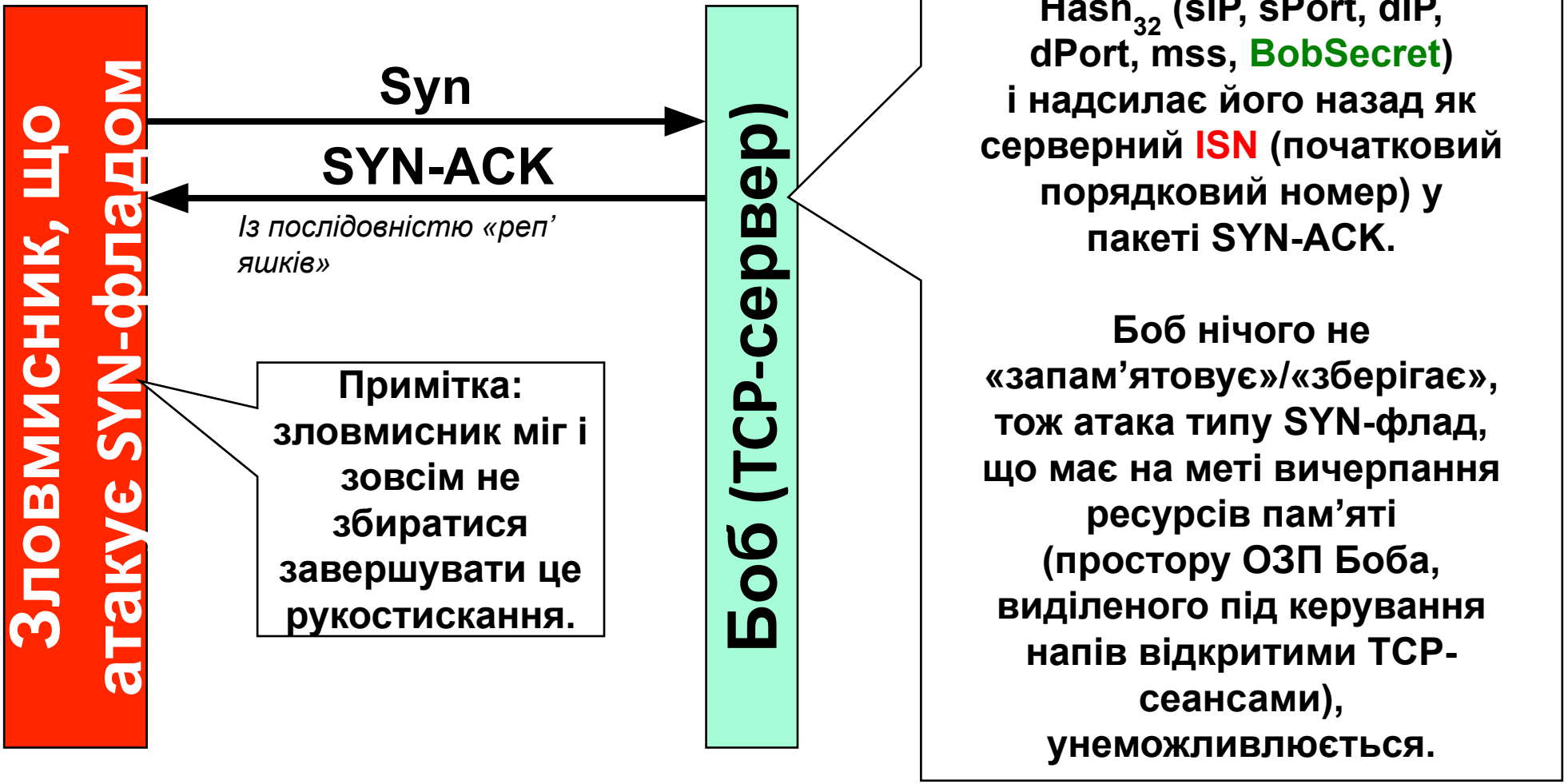


Боб обчислює Hash32 (sIP, sPort, dIP, dPort, mss, BobSecret) і надсилає його назад Алісі як серверний ISN (початковий порядковий номер) у пакеті SYN-ACK. Бобові нема потреби «запам'ятовувати»/«зберігати» що-небудь.

Насправді Боб не розпочинає/створює TCP-сеанс, доки Аліса не дасть коректну відповідь (якщо взагалі дасть) ACK ISN+1» у 3-й частині 3-етапного рукостискання TCP.

Поміркуйте про це!

SYN cookies (Реалізація розд. 4.6.3.2)



SYN cookies (Реалізація розд. 4.6.3.2)

- Зверніть увагу на «конструкцію» власне SYN cookie.
- Це — хеш-сума:
  - пари сокетів (що визначає кінцеві точки),
  - mss (максимального розміру сегмента),
  - деякого секрету, вибраного сервером:
    - на практиці він має періодично змінюватися;
    - це єдина річ, яку сервер насправді пам'ятає, але для всіх спроб з'єднання вона лише одна.
- Цей метод хешування чогось із секретом відомий як MAC (автентифікаційний код повідомлення) або MIC (код _____ повідомлення) і широко використовується в різноманітних прикладних програмах шифрування/автентифікації.

SYN cookies (Реалізація розд. 4.6.3.2)

- Нумо пересвідчимося, що ви вхопили суть.
  - З. Що сервер має пам’ятати/зберігати для кожного ініційованого з’єднання без SYN cookies?
  - В. IP-адресу та порт відправника, а також ISN (початковий порядковий номер).
  - З. Що сервер має пам’ятати/зберігати для кожного ініційованого з’єднання із SYN cookies?
  - В. Тільки поточний _____.
  - З. Чому серверу не потрібно пам’ятати/зберігати нічого, окрім поточного секрету?
  - В. Тому що вся інформація, потрібна для підтвердження того, що частини 1 і 2 3-етапного рукостискання відбулися, _____.

Аналіз трафіка №9

```
popper.net.0 > 192.168.2.7.110: SF 5466905:5466905 (0) win 512
popper.net.0 > 192.168.2.27.110: SF 5466905:5466905 (0) win 512
popper.net.0 > 192.168.2.117.110: SF 5466905:5466905 (0) win 512
popper.net.0 > 192.168.2.21.110: SF 5466905:5466905 (0) win 512
popper.net.0 > 192.168.2.44.110: SF 5466905:5466905 (0) win 512
popper.net.0 > 192.168.2.70.110: SF 5466905:5466905 (0) win 512
. . .
```

- **«Аномальне» використання прапорців _____ і _____ разом.**
- **Навіщо використовувати обидва прапорці? _____.**
- **Зверніть увагу на нелогічний номер порту джерела (0), також доволі часто можна бачити використання номера порту _____.**
- **Як це називається? _____**
- **Це вертикальне чи горизонтальне сканування? _____**

Аналіз трафіка №10

```
07:09:41.2332 stealth.com.51227 > victim.org.23 F 0:0 (0) win 4096
07:09:41.2336 stealth.com.51227 > victim.org.21 F 0:0 (0) win 4096
07:09:41.2341 stealth.com.51227 > victim.org.17 F 0:0 (0) win 4096
07:09:41.2345 stealth.com.51227 > victim.org.53 F 0:0 (0) win 4096
07:09:41.2350 stealth.com.51227 > victim.org.69 F 0:0 (0) win 4096
07:09:41.2354 stealth.com.51227 > victim.org.20 F 0:0 (0) win 4096
. . .
```

- Що одразу виглядає «не так» у цьому трасуванні?

  _____

  _____

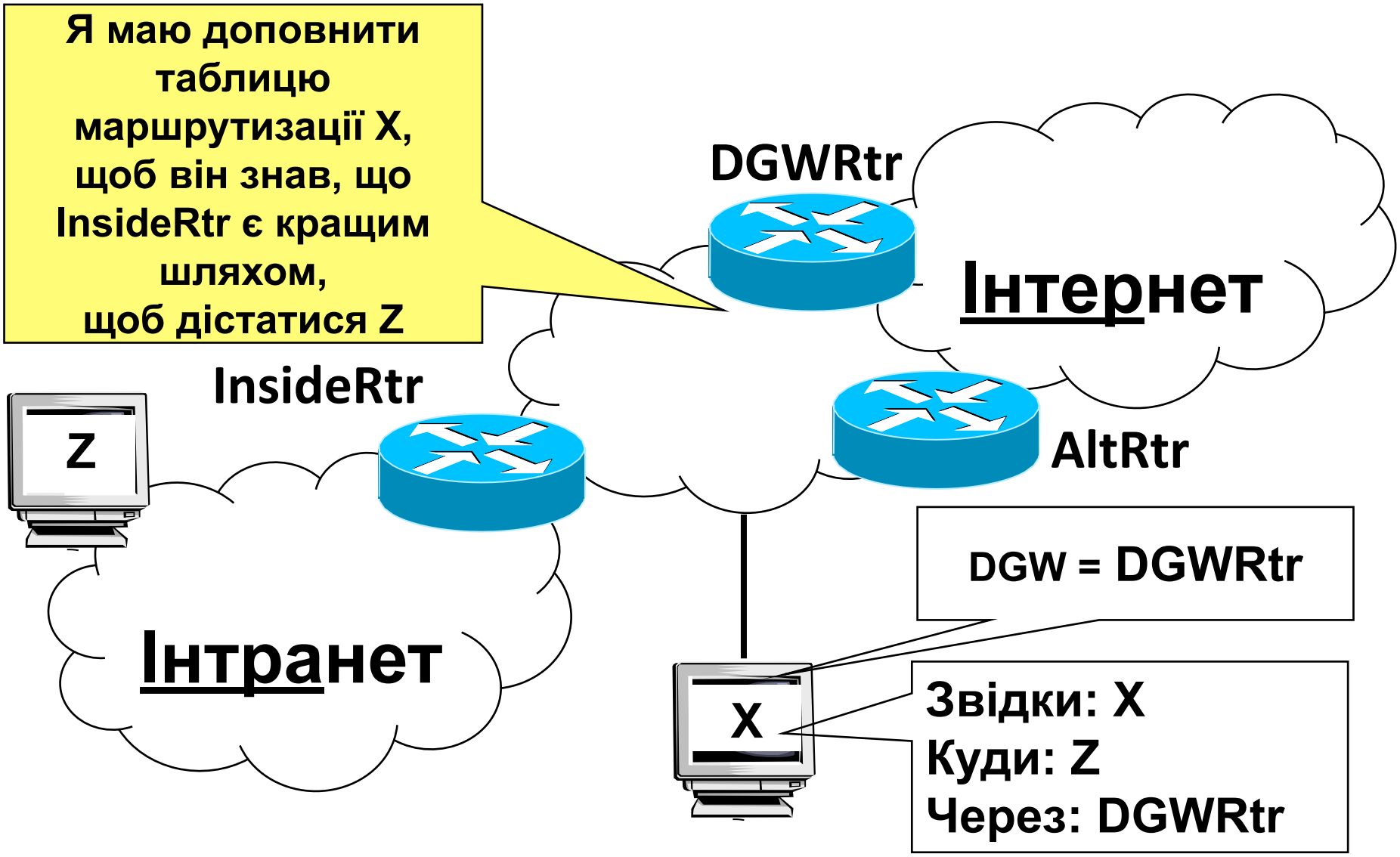
- Якщо жертва відповідає «ACK RST», то _____.
- Це називається _____.
- Воно вертикальне чи горизонтальне? _____

Аналіз трафіка №11

```
13:37:25.310882 tracer.net.2841 > myhost.com.53 udp 36 (ttl 1)
13:37:25.310956 tracer.net.2856 > myhost.com.53 udp 36 (ttl 2)
13:37:25.311080 tracer.net.2814 > myhost.com.53 udp 36 (ttl 4)
13:37:25.311233 tracer.net.2876 > myhost.com.53 udp 36 (ttl 3)
13:37:25.311590 tracer.net.2883 > myhost.com.53 udp 36 (ttl 5)
13:37:25.312066 tracer.net.2840 > myhost.com.53 udp 36 (ttl 6)
. . .
```

- Що найбільш «очевидне» в цьому трасуванні? _____
- Але чому UDP, а не ICMP? _____
- Як змінилася поведінка за промовчанням? _____
  _____
- Що отримує зловмисник? _____

Перенаправлення ICMP (навіщо воно?)

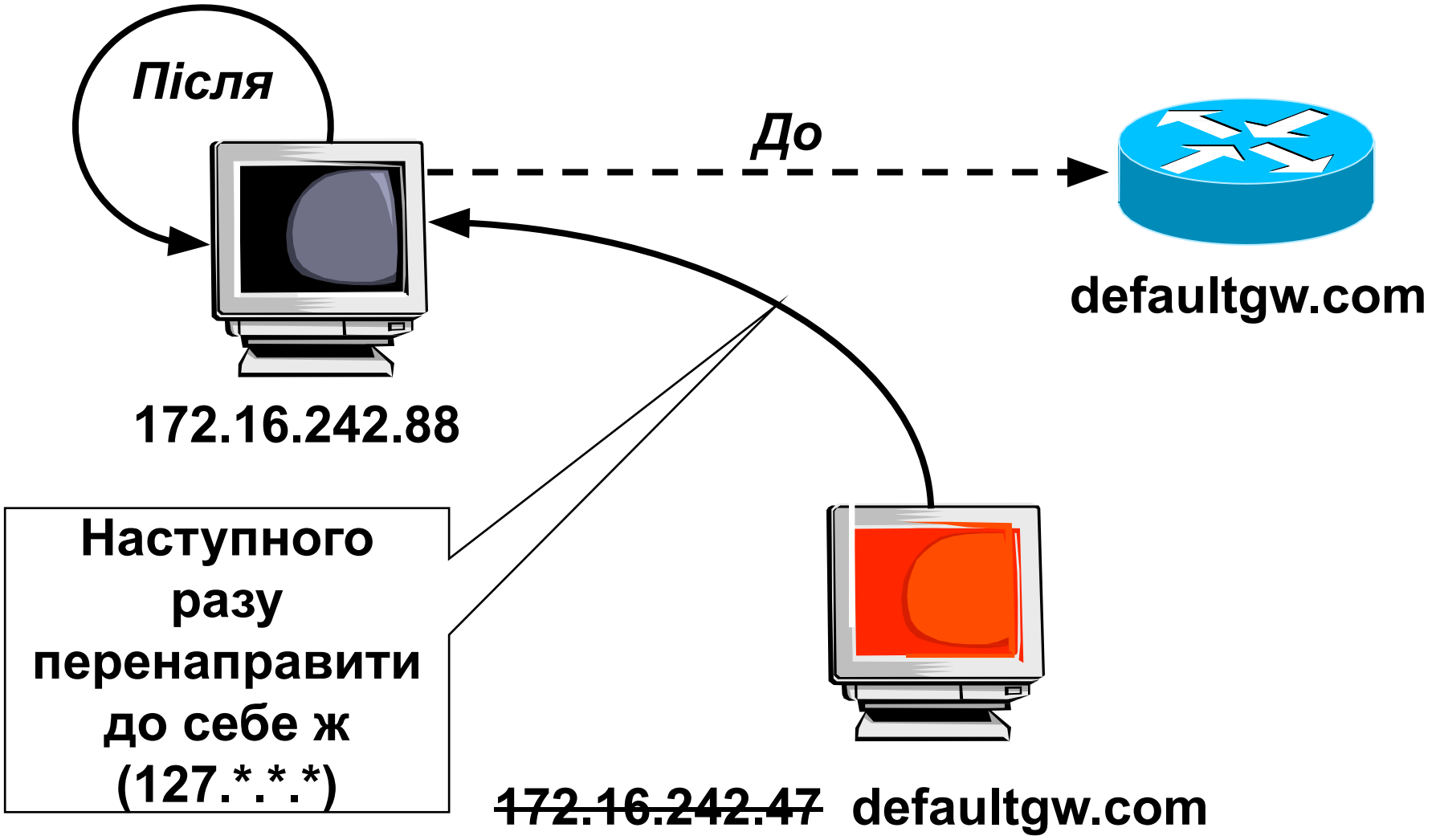


Аналіз трафіка №12

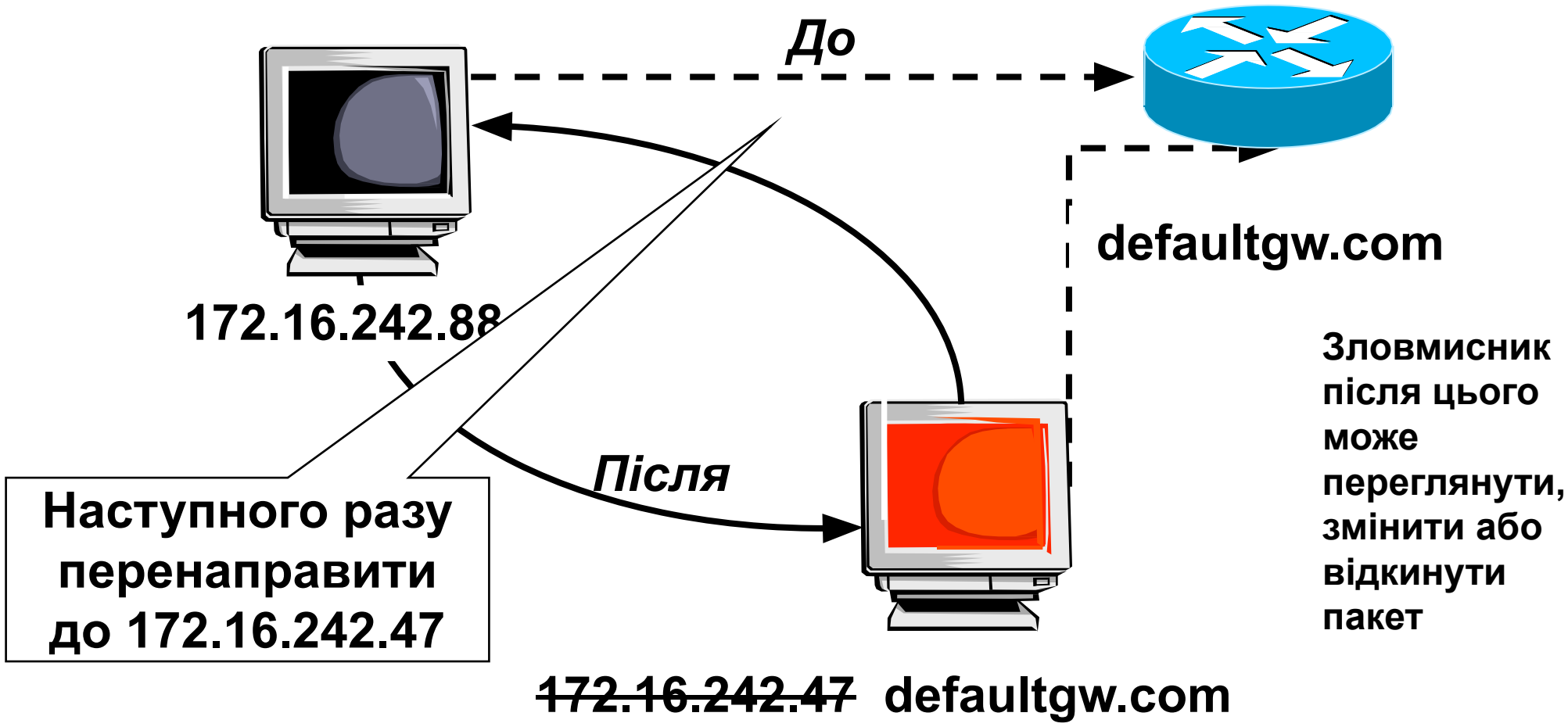
```
16:21:36.650321 defaultgw.com > 130.108.2.17: icmp redirect
16:21:36.650746 defaultgw.com > 130.108.2.27 : icmp redirect
16:21:36.651019 defaultgw.com > 130.108.2.35 : icmp redirect
16:21:36.651562 defaultgw.com > 130.108.2.9 : icmp redirect
16:21:36.651809 defaultgw.com > 130.108.2.102 : icmp redirect
. . .
```

- Не дуже інформативно без вмісту ICMP.
- Втім, з типу повідомлення перенаправлення нам відомо, що вміст має містити IP-адресу _____ _____.
- Зловмисник може вдатися підміни, щоб створити проблеми, тож розглянемо два приклади.

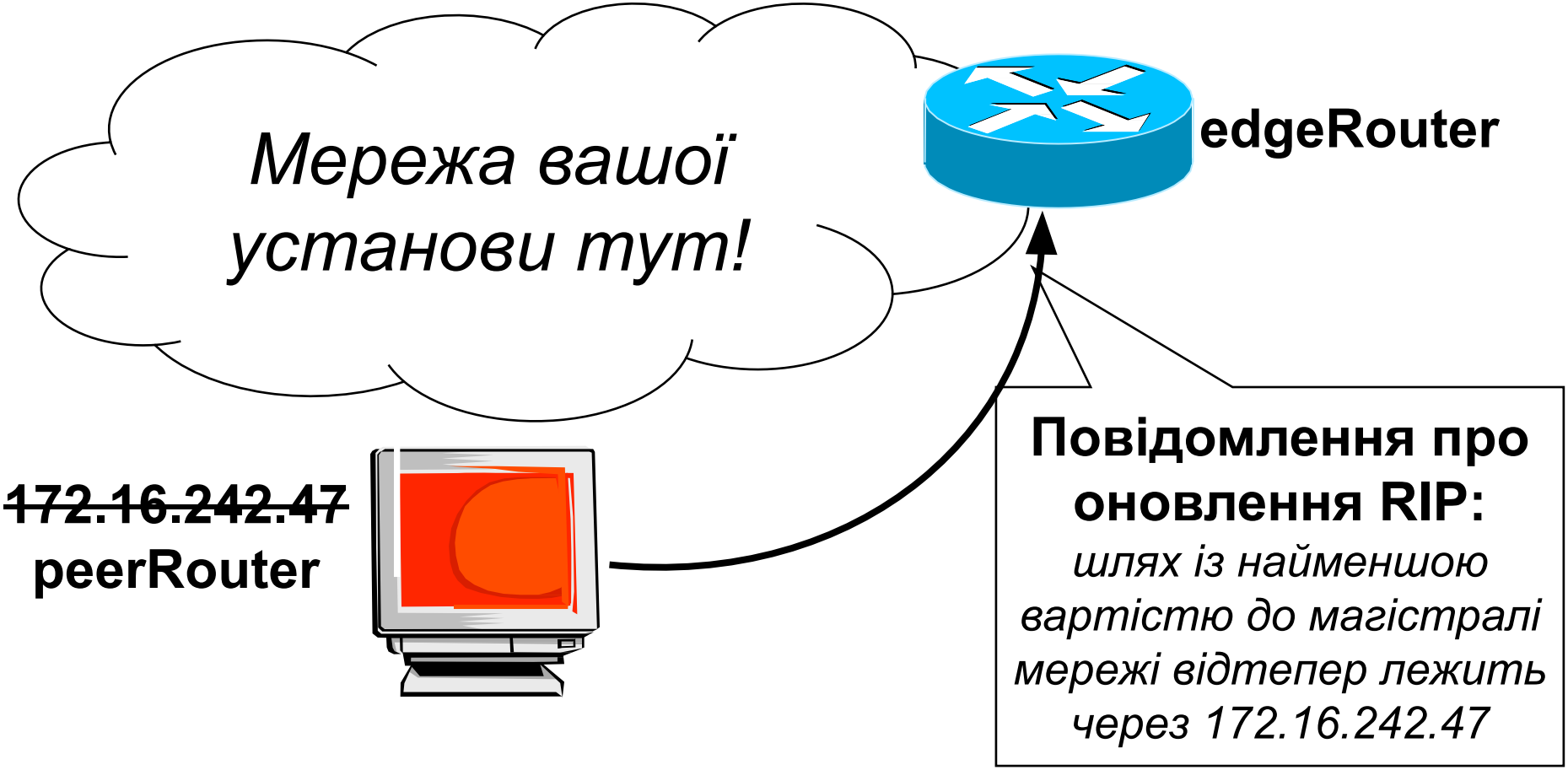
Аналіз трафіка №12-1



Аналіз трафіка №12-2



Схожа («обманна») концепція



Як запобігти виникненню подібної нісенітниці?

Аналіз трафіка №13

02:05:42.980432 middle.com.23 > 195.84.17.243.1624: S 2008278732:2008278732 (0) ack 423384703 win 8192

02:05:43.106781 195.84.17.243.1624 > middle.com.23: R 6073214380:6073214380 (0) ack 2008278733

02:08:18.200476 middle.com.23 > 195.84.17.89.1624: S 2008278732:2008278732 (0) ack 423384703 win 8192

02:08:18.443190 195.84.17.89.1624 > middle.com.23: R 45083302038: 45083302038 (0) ack 2008278733

02:10:02.681277 middle.com.23 > 195.84.17.63.1624: S 2008278732:2008278732 (0) ack 423384703 win 8192

02:13:52.110206 middle.com.23 > 195.84.17.118.1624: S 2008278732:2008278732 (0) ack 423384703 win 8192

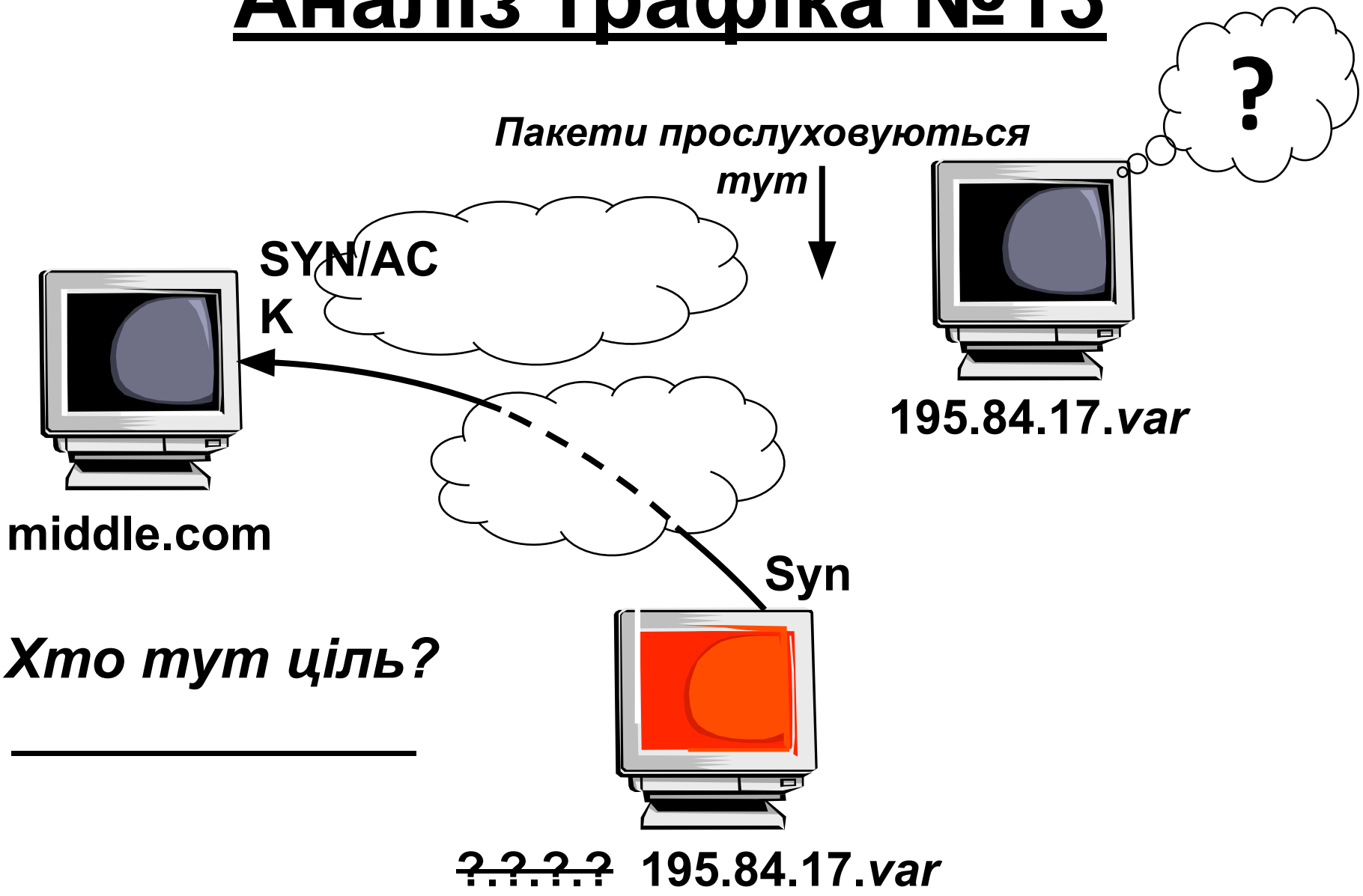
…

Аналіз трафіка №13

Стосовно попереднього слайда…

- **Який прапорець (чи прапорці) встановлюються в пакетах від middle.com? _____**
- **Який прапорець (чи прапорці) встановлюються в пакетах від 195.84.17.*? _____**
- **І при цьому жодних ініціацій SYN з будь-якої адреси 195.84.17.*?**
- **Чи може це бути скануванням? _____ (Підказка: чи це 1-до-багатьох, чи багато-до-1?)**
- **Якщо це ДІЙСНО сканування:**
  - **Чи воно вертикальне, чи горизонтальне? _____**
  - **Як, на вашу думку, його слід назвати? _____**
- **Що ще могло б пояснити цю аномалію? □ наступний слайд**

Аналіз трафіка №13



Аналіз трафіка №13

- Як щодо часових інтервалів між Syn-пакетами від зловмисника (судячи з інтервалів відповідей SYN-ACK від middle.com)?

  _____

- Чи сильніше схиляє вас довгий інтервал до думки, що це шкідлива дія, чи менше? _____
- Чи може зловмисник також здійснювати атаку підміною в інших просторах IP-адрес на додачу до 195.84.17.*? _____
- Окрім швидкості, що ще знижує ефективність атаки Syn-фладу в цьому прикладі?

  _____

Визначення «відбитків» ОС

- Зловмисник може надсилати нормальні чи аномальні пакети («мутанти») до системи в пошуках відповідей, специфічних для певної операційної системи (ОС).
- Більше на цю тему див за адресою: www.insecure.org/nmap/nmap-fingerprinting-article.html.
- Може здійснюватися як пасивно, так і активно.

Пасивне визначення «відбитків» ОС (приклад)

Syn-пакети містять деяку вельми достовірну інформацію щодо ідентифікації ОС.

	Linux	Solaris	WinX	OpenBSD	AIX
Довжина заголовка IP + TCP*	60 Б	44 Б	48 Б	64 Б	44 Б
IP: TTL	64	255	128	64	64
IP: номери наступних ідентифікаторів	Довільні, доки не визначені, після чого +1	+1 увесь час	+1 увесь час	Всі довільні	+1 увесь час
К-ість Syn («привітань»), яку ОС спробує надіслати	5	?	3	4	?
TCP: початковий розмір вікна	5840 або 32 120	8760	16 384	16 384	16 384

*Довжина є функцією того, які параметри TCP задані, які у свою чергу самі є ще одним джерелом ідентифікаційної інформації.

Активне визначення «відбитків» ОС

- **Ключова ідея з точки зору зловмисника:**
  - **завести собі копії кожної версії кожної ОС і запустити їх в ізольованому лабораторному середовищі;**
  - **випробувати на кожній із них різні «стимули», наприклад:**
    - **задати підробні комбінації TCP-прапорців;**
    - **встановити один чи більше лівих 4 бітів «зарезервованого» поля TCP в «1» (на противагу стандартному/очікуваному «0»);**
    - **проявити фантазію, спробувати творчі підходи;**
  - **застосувати результати на реальних цільових машинах.**
  - **Це і є спеціалізацією інструмента NMAP.**
  - **Чи ви чули коли-небудь про «фаззінг»? <обговорення>**

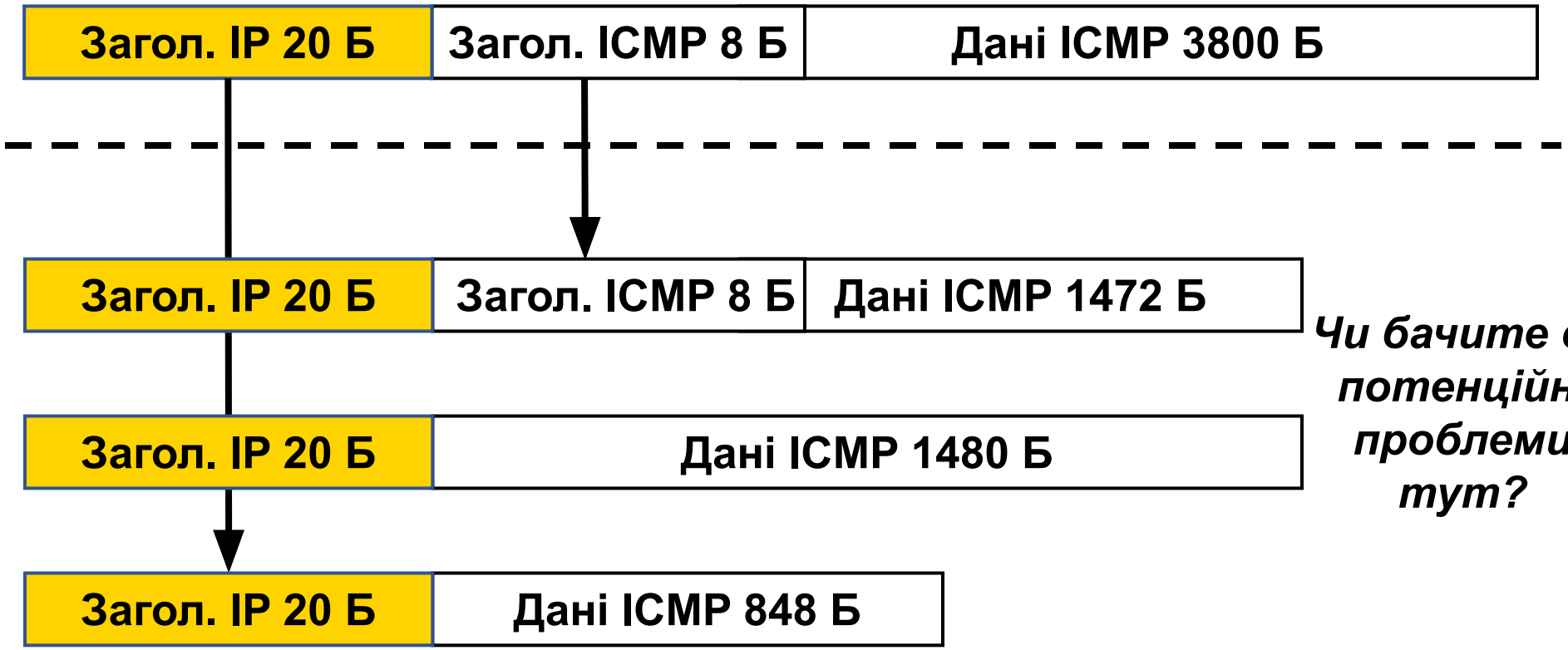
Фрагментація

- Зловмисник може користуватися/зловживати фрагментацією для приховування шкідливих пакетів.
- _____ атаки може бути розбита на кілька дейтаграм.
  - Чи виявить IDS атаку?
  - Чи спрацює коректно визначення та блокування маршрутизаторів із фільтрацією пакетів/міжмережевих екранів?

Фрагментація

Фрагментація

Припустимо, що цей пакет потрапляє до мережі із MTU 1500



Чи бачите ви потенційні проблеми тут?

Фрагментація

- **Повертаючись до попереднього слайда, припустимо, що ми хочемо заборонити весь ICMP-трафік за допомогою пристрою, який *не фіксує стан*.**
  - **Чи не буде в пристрою проблем із фільтруванням першого фрагмента? _____**
  - **Чи не буде в пристрою проблем із фільтруванням 2-го і 3-го фрагментів? _____**
    _____
- **Якщо ми хочемо заборонити всі ICMP-запити на маску підмережі за допомогою пристрою, який *не фіксує стан*?**
  - **Чи не буде яких-небудь проблем із першим фрагментом?**
    _____
  - **А проблем із 2-гими 3-м фрагментами? _____**
    _____

Фрагментація

- **Що пристрій має робити із 2-м і 3-м фрагментами в цьому випадку (внизу попереднього слайда)?**
  - **Переслати їх далі?**
    - **Яка тут проблема? _____**
      _____
  - **Відкинути/заблокувати їх?**
    - **А що щодо порядку надходження? _____**
      _____
    - **Таким чином, потрібна фіксація стану. _____**
      _____

Фрагментація

- **Чи буде система запобігання проникненням (IPS), здатна перевіряти корисне навантаження для виявлення шкідливих сигнатур, працювати, якщо вона бачитиме окремі фрагменти порізно?**

  _____

- **Що IPS має зробити, щоб «виправити» це?**

  _____

  _____

- **Що після цього може зробити зловмисник, щоб скористатися цим?** _____

  _____

  _____

Поля заголовка IP

- Версія: наразі — 4.
- Довжина заголовка: к-ість 32-бітних слів у заголовку.
- Загальна довжина: к-ість байтів у всьому пакеті; макс. 65 535 ($2^{16} – 1$).

Аналіз трафіка №14

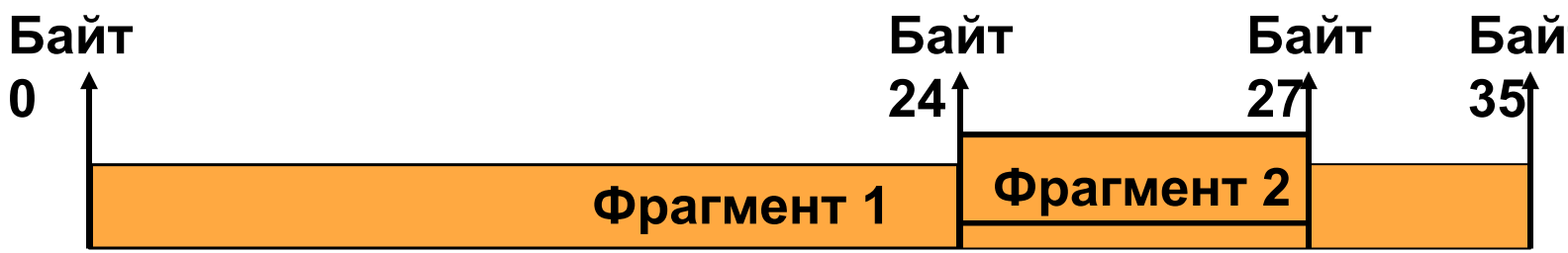
```
evilping.com > victimhost.com: icmp: echo request (frag  56980:
    1480 @ 0 + )
evilping.com  >  victimhost.com:  (frag  56980:  1480  @  1480  +  )
evilping.com  >  victimhost.com:  (frag  56980:  1480  @  2960  +  )
evilping.com  >  victimhost.com:  (frag  56980:  1480  @  4440  +  )
evilping.com  >  victimhost.com:  (frag  56980:  1480  @  5920  +
)

…
evilping.com  >  victimhost.com:  (frag  56980:  1480  @  62160  +  )
evilping.com  >  victimhost.com:  (frag  56980:  1480  @  63640  +  )
evilping.com  >  victimhost.com:  (frag  56980:  1480  @  65120  +
)
```

- **Максимальний розмір IP-пакета — _____.**
- **Що відбувається? _____**

Аналіз трафіка №15

```
evilfrag.com.139 > target.net.139: udp 28 (frag
  242:36 @ 0 +)
evilfrag.com > target.net: (frag 242:4@24)
```



- Це називається атакою «_____».
- Старі системи, що давно не отримували оновлень, можуть «падати», «зависати» чи перезавантажуватися, оскільки вони не знають, як поводитися з цим аномальним станом.

ICMP як прихований канал

- **ICMP може використовуватися як прихований канал між «клієнтом»-зловмисником і багатьма його розподіленими «демонами» (як-от *троянами* чи *зомбі*).**
- **Проблема в тому, що «корисне навантаження» ICMP зазвичай не перевіряється, і ICMP користується свободою «загального доступу» в багатьох мережах.**
- **Таким чином, зловмисне використання ICMP не обмежується атаками скануванням і DoS — його можна використовувати для «тунелювання» команд та аргументів від клієнта («хазяїна») демонам.**

ICMP як прихований канал

Клієнт Loki

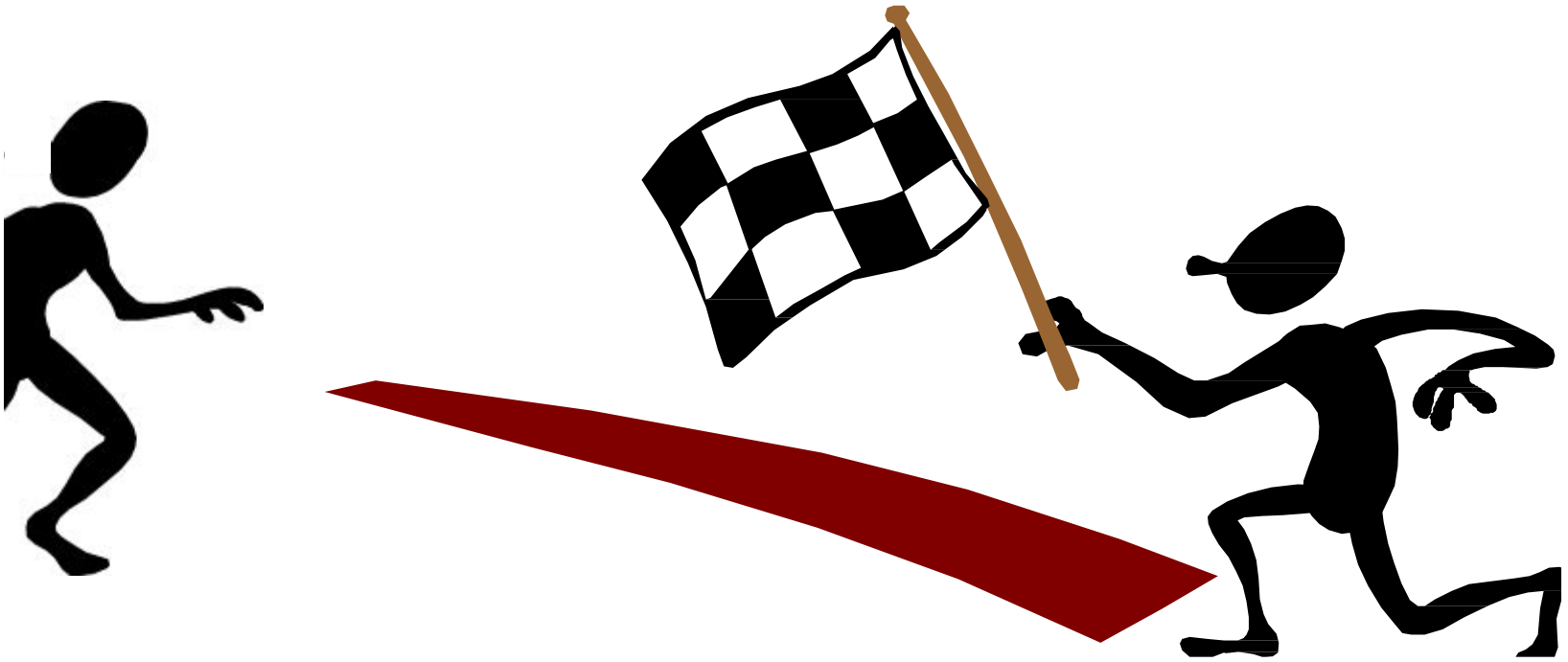
Виглядає безневинно, але ідентифікаційний номер IP можна використати для кодування команд (наприклад, SYN-фладу), а корисне навантаження ICMP може містити аргументи (наприклад, «IP-адреса:порт» цілі).

Хост, на який було встановлено сервер (демон) Loki… якимось чином

ICMP як прихований канал

- Приклад реалізації Loki — атака «Tribe Flood Network» (TFN).
- http://www.cert.org/incident notes/IN-99-07.html
- Схоже на атаку «Smurf» з такими відмінностями:
  - зловмисник, що здійснює атаку «Smurf», використовує проміжні хости лише як «підсилювачі», жодного коду на них не встановлюється;
  - зловмисник, що здійснює атаку TFN, надсилає команди проміжним хостам, «інфікованим» програмою-демоном TFN.

Кінець



Додаткова практика з шістнадцятковим поданням

<4500 002c b5cb 21e6 6806 c229 0d12 3e0a 0d12 3f02> [22b4 0050 391f 8c4d aa45 2176 6012 0fb7 26e6 d5f0 0400 0000] { }

8 запитань нижче ґрунтуються на пакеті, наведеному вище. Він повторюється на кожному слайді для зручності.
Коли ви будете готові перевірити свої відповіді, перейдіть до останнього слайда.

Практика з шістнадцяткового аналізу пакетів

<4500 002c b5cb 21e6 6806 c229 0d12 3e0a 0d12 3f02> [22b4 0050 391f 8c4d aa45 2176 6012 0fb7 26e6 d5f0 0400 0000] { }

Припустимо, ви вже знаєте, що це пакет IPv4.

31. Який протокол інкапсульований (тобто переноситься) в цьому заголовку IP?

B1. _____

Практика з шістнадцяткового аналізу пакетів

<4500 002c b5cb 21e6 6806 c229 0d12 3e0a 0d12 3f02> [22b4 0050 391f 8c4d aa45 2176 6012 0fb7 26e6 d5f0 0400 0000] { }

32. Схоже, що цей пакет…

a. прямує до вебсервера;

b. надходить від вебсервера;

c. прямує до DNS-сервера;

d. надходить від DNS-сервера.

B2. _____

Практика з шістнадцяткового аналізу пакетів

<4500 002c b5cb 21e6 6806 c229 0d12 3e0a 0d12 3f02> [22b4 0050 391f 8c4d aa45 2176 6012 0fb7 26e6 d5f0 0400 0000] { }

З3. Яке значення TTL пакета в десятковому поданні?

В3. _____

Практика з шістнадцяткового аналізу пакетів

<4500 002c b5cb 21e6 6806 c229 0d12 3e0a 0d12 3f02> [22b4 0050 391f 8c4d aa45 2176 6012 0fb7 26e6 d5f0 0400 0000] { }

34. У цьому пакеті…

a. задано 0 IP- і 0 TCP-параметрів;

b. задано > 0 IP-, але 0 TCP-параметрів;

c. задано 0 IP-, але > 0 TCP-параметрів;

d. задано > 0 IP- і > 0 TCP-параметрів.

B4. _____

Практика з шістнадцяткового аналізу пакетів

<4500 002c b5cb 21e6 6806 c229 0d12 3e0a 0d12 3f02> [22b4 0050 391f 8c4d aa45 2176 6012 0fb7 26e6 d5f0 0400 0000] { }

35. Якщо припустити, що зазначені IP-адреси належать до мережі /24, чи перебувають обидві ці машини в одній мережі?

B5. _____

Практика з шістнадцяткового аналізу пакетів

<4500 002c b5cb 21e6 6806 c229 0d12 3e0a 0d12 3f02> [22b4 0050 391f 8c4d aa45 2176 6012 0fb7 26e6 d5f0 0400 0000] { }

36. Цей пакет…

a. не фрагментований;

b. є першим фрагментом;

c. є «середнім» фрагментом;

d. є останнім фрагментом.

B6. _____

Практика з шістнадцяткового аналізу пакетів

<4500 002c b5cb 21e6 6806 c229 0d12 3e0a 0d12 3f02> [22b4 0050 391f 8c4d aa45 2176 6012 0fb7 26e6 d5f0 0400 0000] { }

37. Який прапорець (чи прапорці) заданий у заголовку TCP?

B7. _____

Практика з шістнадцяткового аналізу пакетів

<4500 002c b5cb 21e6 6806 c229 0d12 3e0a 0d12 3f02> [22b4 0050 391f 8c4d aa45 2176 6012 0fb7 26e6 d5f0 0400 0000] { }

38. Який параметр TCP заданий?

B8. _____

Відповіді на практичні запитання

В1. TCP. Погляньте на байт із зсувом 9 і ви побачите «06», що є призначеним для TCP номером.

В2. «A». Порт призначення (не джерела) — 5016, тобто 8010 (5 × 16 + 0 × 1), який пов'язаний із вебслужбою.

В3. 104. Знайдіть поле TTL у байті зі зсувом 8 і ви побачите там 6816, тобто 10 410 (6 × 16 + 8 × 1).

В4. «C». Поле довжини заголовка (IHL) IP (права половина байта 0) містить 5 (min), а поле зсуву TCP (ліва половина байта 12) — 6 (min + 1).

В5. Ні. Обидві адреси містяться в останніх 8 байтах заголовка IP. Якщо подивитися на лише перші 3 октети (/24) кожної адреси, то можна побачити, що 0d123e не дорівнює 0d123f.

Відповіді на практичні запитання

В6. «С». Інформація про фрагменти міститься у байтах 6 і 7 — це значення 21e6, або 0010000111100110. Оскільки прапорець MF установлений в «істину», і зсув фрагмента не дорівнює нулю, це «середній» фрагмент.

В7. SYN і ACK. Прапорці TCP знаходяться у байті 13. Значення байта 13 — 1216, у двійковому поданні — 0001 0010. З цих 8 бітів прапорці — 6 бітів праворуч, тобто 010010. Два біти, що «встановлені» (дорівнюють 1), відповідають прапорцям ACK і SYN.

В8. Вибіркове підтвердження ACK (або «SACK» — від «selective ACK»). Параметри (якщо вони задані в заголовку TCP) йдуть одразу слідом за обов'язковою частиною (перші 20 байтів) заголовка TCP. Подивившись туди (тобто на байт зі зсувом 20), ми побачимо 416, тобто 410, що відповідає SACK.