Минобрнауки России
Федеральное государственное бюджетное образовательное
учреждение высшего образования
НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМ. Р.Е. АЛЕКСЕЕВА
ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ

Курс “Сети и телекоммуникация”

Отчет по лабораторной работе №6

Выполнил: Соков С.А.
Проверил: Гай В.Е.

Нижний Новгород 2021

Задание:

1. Перехватить udp (icmp, tcp) пакет
2. Рассчитать контрольную сумму заголовка вручную
3. Процесс расчёта привести в отчёте
4. Проверить расчёт контрольной суммы

5. Внести ошибку в заголовок и пересчитать контрольную сумму

Ход работы:

Исходя из заданной во втором слове длине заголовка, мы выделяем байты, которые необходимы нам для расчета.

```
root@n1:/tmp/pycore.45831/n1.conf# tcpdump -c 1 -xx 'dst host 10.0.0.11 and i> tcpdump: verb
ose output suppressed, use -v or -vv for full protocol decode     listening on eth0, link-ty
pe EN10MB (Ethernet), capture size 262144 bytes
11:58:29.368753 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 41, seq 1, length 64
        0x0000:  0000 00aa 0001 0000 00aa 0000 0800 4500
        0x0010:  0054 63f3 0000 4001 02a2 0a00 000a 0a00
        0x0020:  000b 0000 162f 0029 0001 35d3 a460 0000
        0x0030:  0000 4ba0 0500 0000 0000 1011 1213 1415
        0x0040:  1617 1819 1a1b 1c1d 1e1f 2021 2223 2425
        0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435
        0x0060:  3637
```

4500	0054
63F3	0000
4001	0000
0A00	000A
0A00	000B

Расчет контрольной суммы:

1. Разбиваем заголовок с обнуленным полем контрольной суммы на слова по 16 бит и суммируем полученные 16-битные слова между собой:

$(4500)_{16} + (0054)_{16} + (63F3)_{16} + (0000)_{16} + (4001)_{16} + (0000)_{16} + (0A00)_{16} + (000A)_{16} + (0A00)_{16} + (000B)_{16} = (FD5D)_{16}$

2. Находим контрольную сумму, как двоичное поразрядное дополнение результата сложения:
$CSIP = (FFFF)_{16} - (FD5D)_{16} = (02A2)_{16}$.

Проверка контрольной суммы:

1. Суммируем все 16-битные слова заголовка между собой:

$(4500)_{16} + (0054)_{16} + (63F3)_{16} + (0000)_{16} + (4001)_{16} + (02A2)_{16} + (0A00)_{16} + (000A)_{16} + (0A00)_{16} + (000B)_{16} = (FFFF)_{16}$

2. Находим двоичное поразрядное дополнение результата сложения:

$(FFFF)_{16}$ - $(FFFF)_{16}$ = $(0000)_{16}$.

Внесем ошибку:

Проверка:

1. Суммируем все 16-битные слова заголовка между собой:

$(4500)_{16}$ + $(0054)_{16}$ + $(63F3)_{16}$ + $(4F3C)_{16}$ + $(4001)_{16}$ + $(02A2)_{16}$ + $(0A00)_{16}$ + $(000A)_{16}$ + $(0A00)_{16}$ + $(000B)_{16}$ = $(14F3B)_{16}$

2. Поскольку результат сложения превышает 16 бит, разбиваем его на два слова по 16 бит каждое и снова их суммируем:

$(0001)_{16}$ + $(4F3B)_{16}$ = $(4F3C)_{16}$.

3. Находим двоичное поразрядное дополнение результата сложения:

$(FFFF)_{16}$ - $(4F3C)_{16}$ = $(B0C3)_{16}$.

Ноль не получился, следовательно проверка не прошла.