

Минобрнауки России

Федеральное государственное бюджетное образовательное

учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ИМ. Р.Е. АЛЕКСЕЕВА

ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Сети и телекоммуникации

Отчет по лабораторной работе №2

Выполнил: Гора К.А.

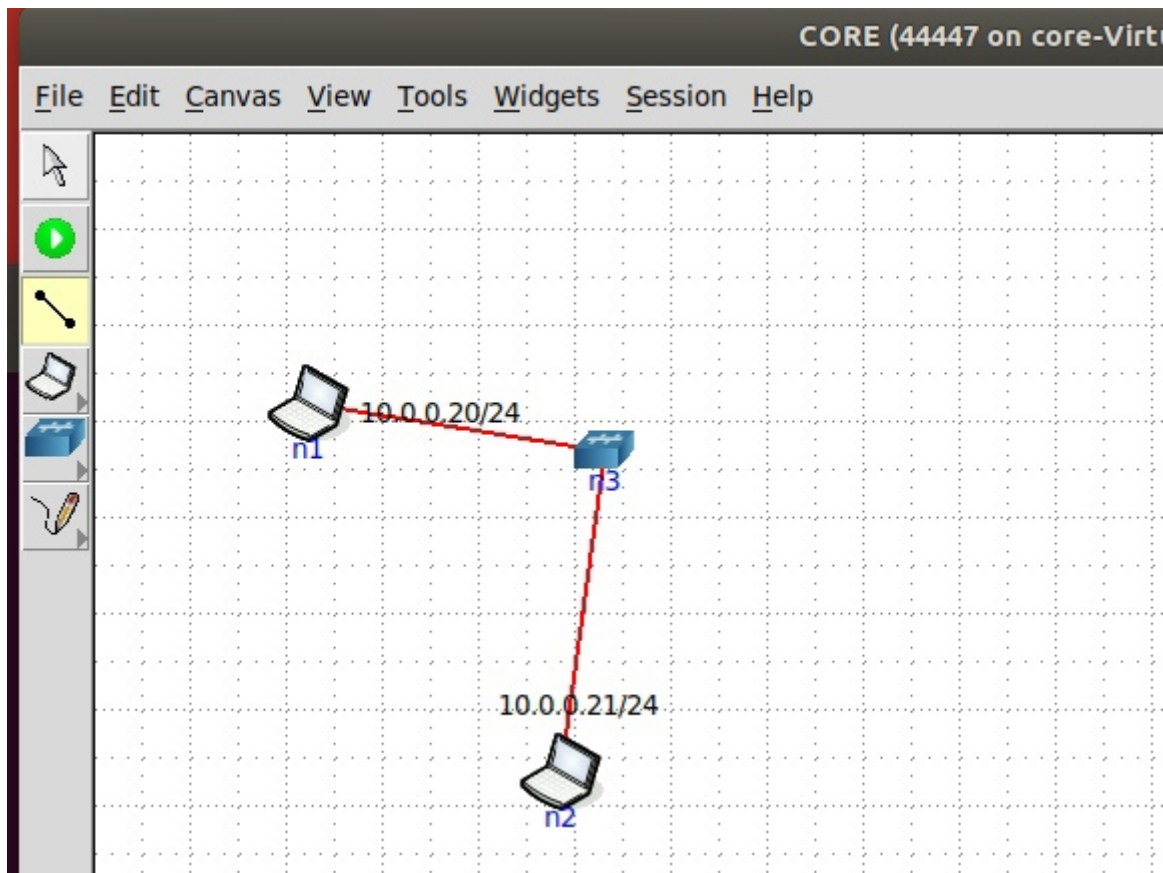
Проверил: Гай В.Е.

Нижний Новгород 2021

Задание на лабораторную работу:

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

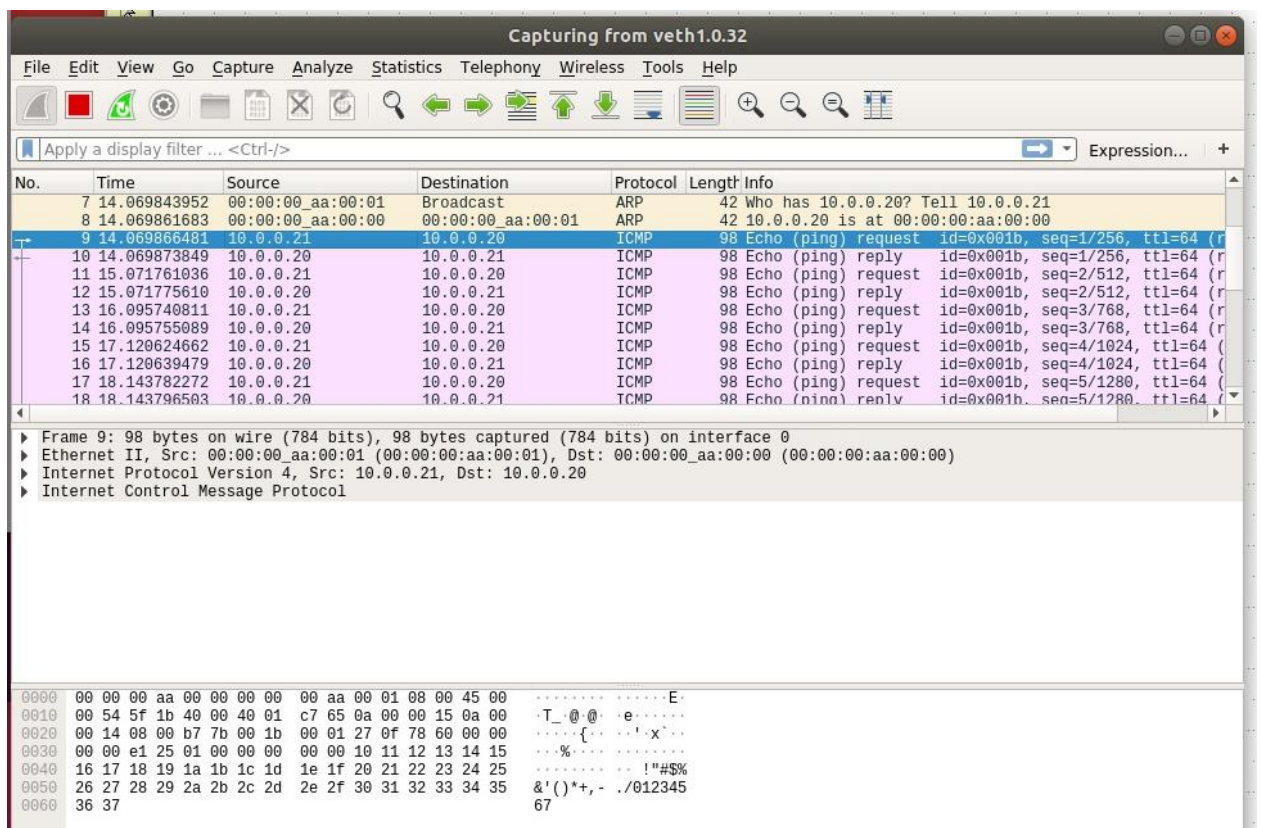
Ход работы:



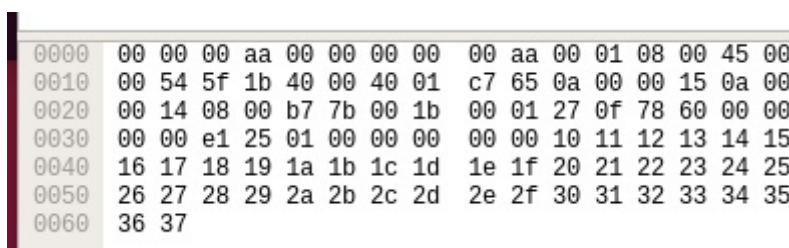
Запустим ping с n2 на n1

```
Файл Правка Вид Поиск Терминал Справка
root@n2:/tmp/pycore.44447/n2.conf# ping 10.0.0.20
PING 10.0.0.20 (10.0.0.20) 56(84) bytes of data.
64 bytes from 10.0.0.20: icmp_seq=1 ttl=64 time=0.058 ms
64 bytes from 10.0.0.20: icmp_seq=2 ttl=64 time=0.045 ms
64 bytes from 10.0.0.20: icmp_seq=3 ttl=64 time=0.043 ms
64 bytes from 10.0.0.20: icmp_seq=4 ttl=64 time=0.045 ms
64 bytes from 10.0.0.20: icmp_seq=5 ttl=64 time=0.043 ms
64 bytes from 10.0.0.20: icmp_seq=6 ttl=64 time=0.047 ms
64 bytes from 10.0.0.20: icmp_seq=7 ttl=64 time=0.044 ms
^C
--- 10.0.0.20 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6122ms
rtt min/avg/max/mdev = 0.043/0.046/0.058/0.008 ms
root@n2:/tmp/pycore.44447/n2.conf#
```

Откроем wireshark выберем пакет.



Рассмотрим кадр Ethernet:



Заголовок IP-пакета:

0000	00	00	00	aa	00	00	00	00	00	aa	00	01	08	00	45	00
0010	00	54	5f	1b	40	00	40	01	c7	65	0a	00	00	15	0a	00
0020	00	14	08	00	b7	7b	00	1b	00	01	27	0f	78	60	00	00
0030	00	00	e1	25	01	00	00	00	00	00	10	11	12	13	14	15
0040	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25
0050	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35
0060	36	37														

Контрольная сумма:

0000	00	00	00	aa	00	00	00	00	00	aa	00	01	08	00	45	00
0010	00	54	5f	1b	40	00	40	01	c7	65	0a	00	00	15	0a	00
0020	00	14	08	00	b7	7b	00	1b	00	01	27	0f	78	60	00	00
0030	00	00	e1	25	01	00	00	00	00	00	10	11	12	13	14	15
0040	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25
0050	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35
0060	36	37														

Параметры ICMP протокола:

0000	00	00	00	aa	00	00	00	00	00	aa	00	01	08	00	45	00
0010	00	54	5f	1b	40	00	40	01	c7	65	0a	00	00	15	0a	00
0020	00	14	08	00	b7	7b	00	1b	00	01	27	0f	78	60	00	00
0030	00	00	e1	25	01	00	00	00	00	00	10	11	12	13	14	15
0040	16	17	18	19	1a	1b	1c	1d	1e	1f	20	21	22	23	24	25
0050	26	27	28	29	2a	2b	2c	2d	2e	2f	30	31	32	33	34	35
0060	36	37														

00 00 00 aa 00 00 – MAC-адрес получателя;

00 00 00 aa 00 01 – MAC-адрес отправителя;

08 00 – код протокола (IP);

Заголовок IP-пакета:

4 – номер версии протокола IP (IPv4);
 5 – длина заголовка (пять 32-битных слов);
 00 – тип сервиса: приоритет пакета (первые три бита) - 0, критерии выбора маршрута (задержка, пропускная способность и надежность) – так же 0;
 00 54 – общая длина IP-пакета;
 5f 1b – идентификатор пакета;
 40 00 – флаги и смещение фрагмента: первые три бита (флаги) – 0 1 0, где 2-й бит – флаг DF, который запрещает маршрутизатору фрагментировать пакет; так как пакет не фрагментируется, поле смещения – 0;
 40 – время жизни пакета (в секундах – 64 с);
 01 – протокол верхнего уровня (ICMP);
 с7 65 – контрольная сумма заголовка;
 0a 00 00 15 – IP-адрес источника
 0a 00 00 14 – IP-адрес назначения

4500	0054
5F1B	4000
4001	0000
0A00	0015
0A00	0014

1) Разбиваем заголовок на слова по 16 бит и суммируем полученные 16-битные слова между собой:

$$(4500)_{16} + (0054)_{16} + (5F1B)_{16} + (4000)_{16} + (4001)_{16} + (0000)_{16} + (0A00)_{16} + (0015)_{16} + (0A00)_{16} + (0014)_{16} = (13899)_{16}$$

2) Поскольку результат сложения в двоичном представлении превышает 16 разрядов (или 4 шестнадцатеричных цифры), разбиваем его на два слова по 16 бит каждое и снова их суммируем:

$$(0001)_{16} + (3899)_{16} = (389A)_{16}$$

3) Находим контрольную сумму, как двоичное поразрядное дополнение результата сложения:

$$CS_{IP} = (FFFF)_{16} - (389A)_{16} = (C765)_{16}$$

Контрольные суммы совпадают.

Проверим корректность контрольной суммы (C765)₁₆

Суммируем все 16-ти битные слова заголовка между собой

$$(4500)_{16} + (0054)_{16} + (5F1B)_{16} + (4000)_{16} + (4001)_{16} + (C765)_{16} + (0A00)_{16} + (0015)_{16} + (0A00)_{16} + (0014)_{16} = (1FFFE)_{16}$$

Поскольку результат сложения в двоичном представлении превышает 16 разрядов (или 4 шестнадцатеричных цифры), разбиваем его на два слова по 16 бит каждое и снова их суммируем:

$$(0001)_{16} + (FFFE)_{16} = (FFFF)_{16}$$

Находим двоичное поразрядное дополнение результата сложения:

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

Внесем ошибку в заголовок и пересчитать контрольную сумму (в идентификатор пакета)

4500	0054
5F1B	4000
4001	0000
0A00	0015
0A00	0014

Проверим корректность контрольной суммы (C765)₁₆

Суммируем все 16-ти битные слова заголовка между собой

$$(4500)_{16} + (0054)_{16} + (2F1B)_{16} + (4000)_{16} + (4001)_{16} + (C765)_{16} + (0A00)_{16} + (0015)_{16} + (0A00)_{16} + (0014)_{16} = (1CFFE)_{16}$$

Поскольку результат сложения в двоичном представлении превышает 16 разрядов (или 4 шестнадцатеричных цифры), разбиваем его на два слова по 16 бит каждое и снова их суммируем:

$$(0001)_{16} + (CFFE)_{16} = (CFFF)_{16}$$

Находим двоичное поразрядное дополнение результата сложения:

$$(FFFF)_{16} - (CFFF)_{16} = (3000)_{16}$$