18+

Иван Андреевич Трещев
Игорь Александрович Кожин

Безопасность вычислительных сетей

Практические аспекты

Иван Трещев

Безопасность вычислительных сетей. Практические аспекты

«Издательские решения»

Трещев И. А.

Безопасность вычислительных сетей. Практические аспекты / И. А. Трещев — «Издательские решения»,

ISBN 978-5-44-989454-0

Книга содержит основные сведения в области безопасности вычислительных сетей. Приведены основные сведения по настройке Ideco ICS, Cisco ASA, ЦУС Континент.

ISBN 978-5-44-989454-0

Содержание

Безопасность вычислительных сетей Практические аспекты

Иван Андреевич Трещев
Игорь Александрович Кожин

Общий анализ Анастасия Сергеевна Ватолина

ISBN 978-5-4498-9454-0
Создано в интеллектуальной издательской системе Ridero

Введение

Использование средств вычислительной техники сегодня не ограничивается выполнением математических расчетов для нужд различных отраслей народного хозяйства.

В настоящее время сложно найти семью в которой не было бы компьютера или другого устройства подключенного ко «всемирной паутине». Вопрос защиты данных в информационных сетях общего пользования является достаточно актуальным и обеспечение конфиденциальности информации сегодня выходит на первый план.

Конфиденциальная переписка, дистанционные технологии взаимодействия в рамках корпоративного общения, проведения семинаров, деловых встреч.

Данная книга скорее содержит общую информацию об обеспечении информационной безопасности в распределенных информационных системах, чем представляет из себя практическое руководство к действию.

Глава 1. Техника и технология сниффинга пакетов

2 Применение сниффера

2.1 Перехват трафика при использовании в сети концентратора

Наиболее опасны снифферы в сетях где циркулирует незашифрованный траффик. Сегодня использование сетей с коммутаторами существенно затрудняет перехват чужого траффик. Коммутатор в зависимости от MAC адреса устройства на его порту не производит широковещание пакетов а целенаправленно отправляет их адресату. сетевой пакет, принадлежащий сети, которая спроектирована с использованием концентраторов. Порой при анализе сетей все же используют концентраторы.

Для проверки уязвимости соберем лабораторный стенд по топологии, представленный на рисунке 1. На атакующем компьютере был установлен сниффер Wireshark, позволяющий перехватывать сетевой трафик для дальнейшего анализа.

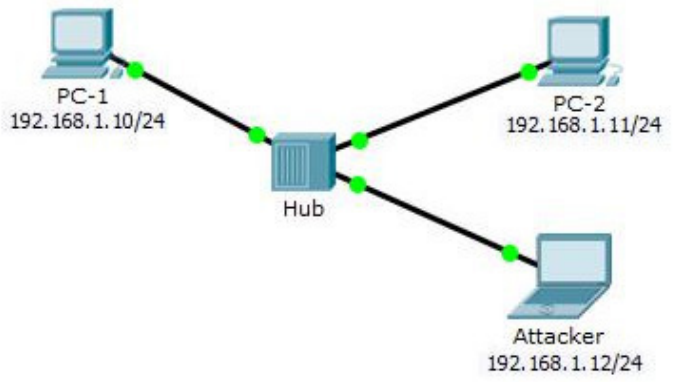


Рисунок 1 – Лабораторный стенд для проверки уязвимости

Компьютеры жертв имеют IPv4-адреса 10.10.1.3 и 10.10.1.4 (рисунки 2 и 3). Между ними будет проходить Echo-запрос посредством ввода команды ping «адрес». Атакующий с запущенным Wireshark должен обнаружить Echo-запросы по пакетам протокола ICMP (Internet Control Message Protocol – протокол межсетевых управляющих сообщений). Это продемонстрировано на рисунке 4.

```
C:\Users\Admin>ping 10.1.3.3

Обмен пакетами с 10.1.3.3 по с 32 байтами данных:
Ответ от 10.1.3.3: число байт=32 время=2мс TTL=128
Ответ от 10.1.3.3: число байт=32 время=1мс TTL=128
Ответ от 10.1.3.3: число байт=32 время=1мс TTL=128
Ответ от 10.1.3.3: число байт=32 время=2мс TTL=128

Статистика Ping для 10.1.3.3:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 2 мсек, Среднее = 1 мсек
```

Рисунок 2 – Echo-запрос от компьютера с адресом 10.1.3.4

```
C:\Users\Admin>ping 10.1.3.4

Обмен пакетами с 10.1.3.4 по с 32 байтами данных:
Ответ от 10.1.3.4: число байт=32 время=1мс TTL=128
Ответ от 10.1.3.4: число байт=32 время=1мс TTL=128
Ответ от 10.1.3.4: число байт=32 время<1мс TTL=128
Ответ от 10.1.3.4: число байт=32 время=1мс TTL=128

Статистика Ping для 10.1.3.4:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек
```

Рисунок 3 – Echo-запрос от компьютера с адресом 10.1.3.3

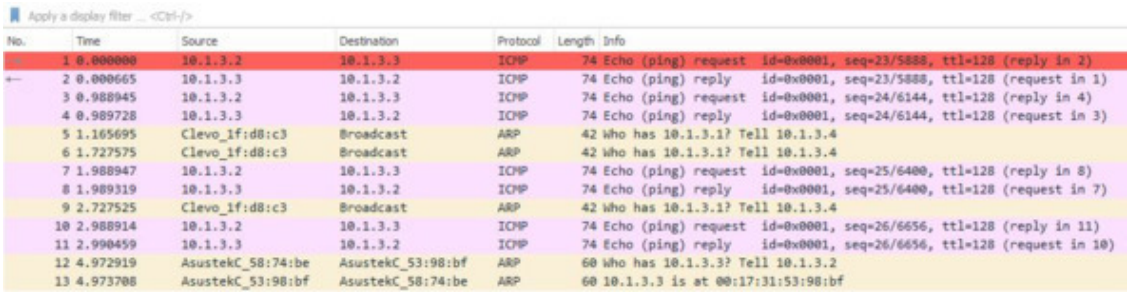


Рисунок 4 – Обнаружение Echo-запросов

2.2 Перехват мультимедийных файлов

Организация атаки на незащищённые серверы SMB является одной из наиболее привлекательных среди злоумышленников. Так, например, с помощью использования уязвимостей протокола SMB были осуществлены взлом серверов Sony Pictures Entertainment и распространение вредоносного ПО DoublePulsar, WannaCry (уязвимость EternalBlue) и Petya.

Сначала настроем протокол SMB2 на компьютерах жертв. Для этого на рабочем столе жертв создали папку «Сетевая папка 1». Вызываем ПКМ контекстное меню папки и выбираем «Свойства». В открывшемся окне во вкладке «Доступ» выбрать «Общий доступ», выбрать пользователя «Все», выставить уровень разрешений «Чтение и запись». Теперь папка будет доступна всем в данной локальной сети (рисунки 5 – 8).

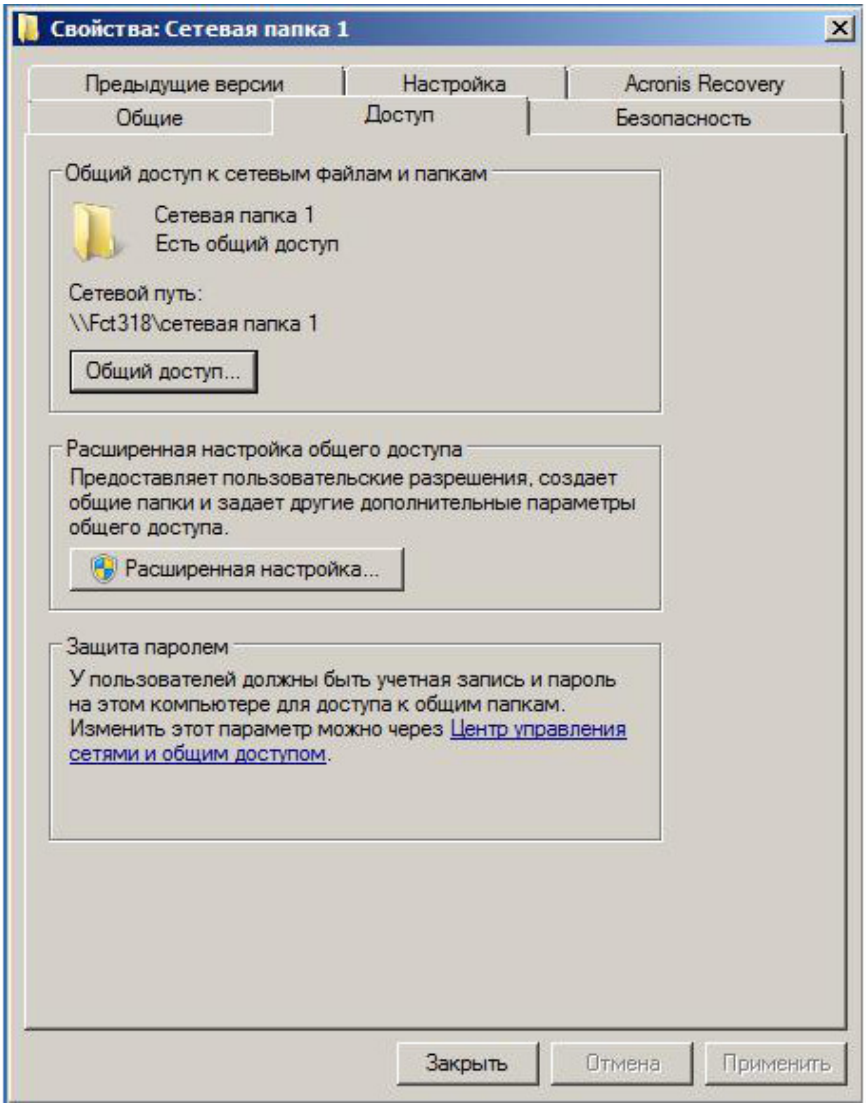


Рисунок 5 – Свойства сетевой папки

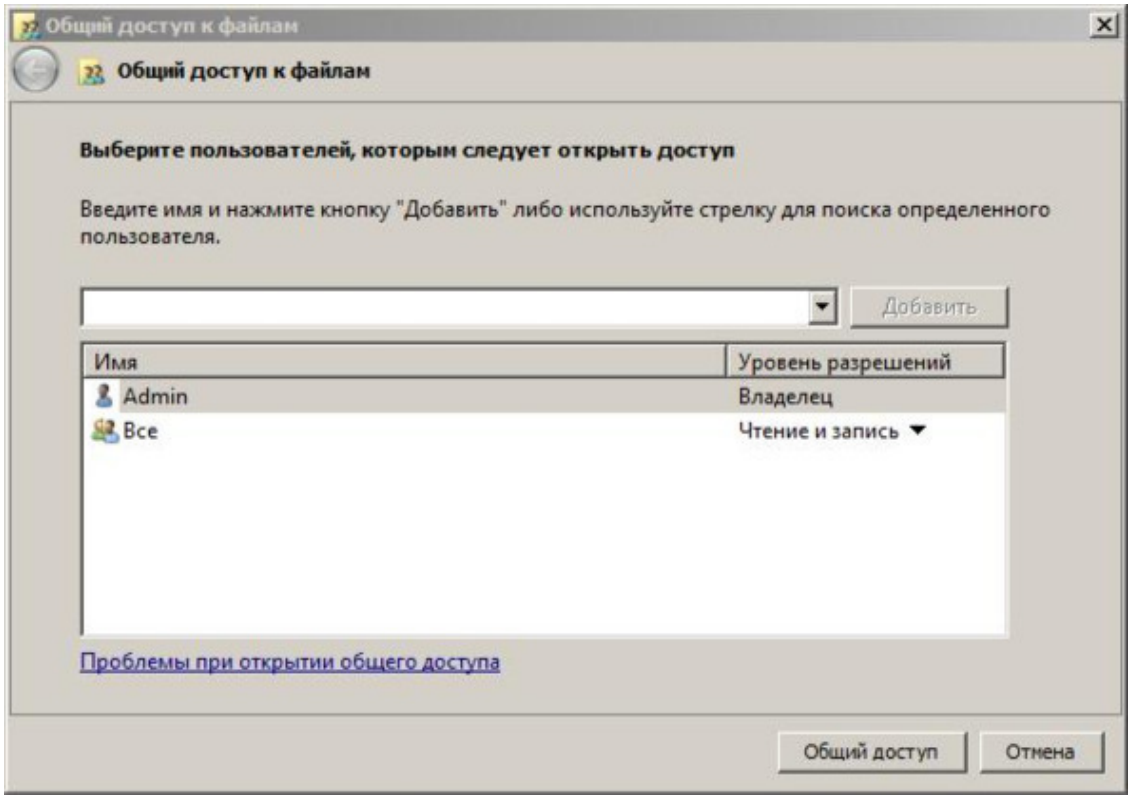


Рисунок 6 – Выбор пользователей для открытия общего доступа

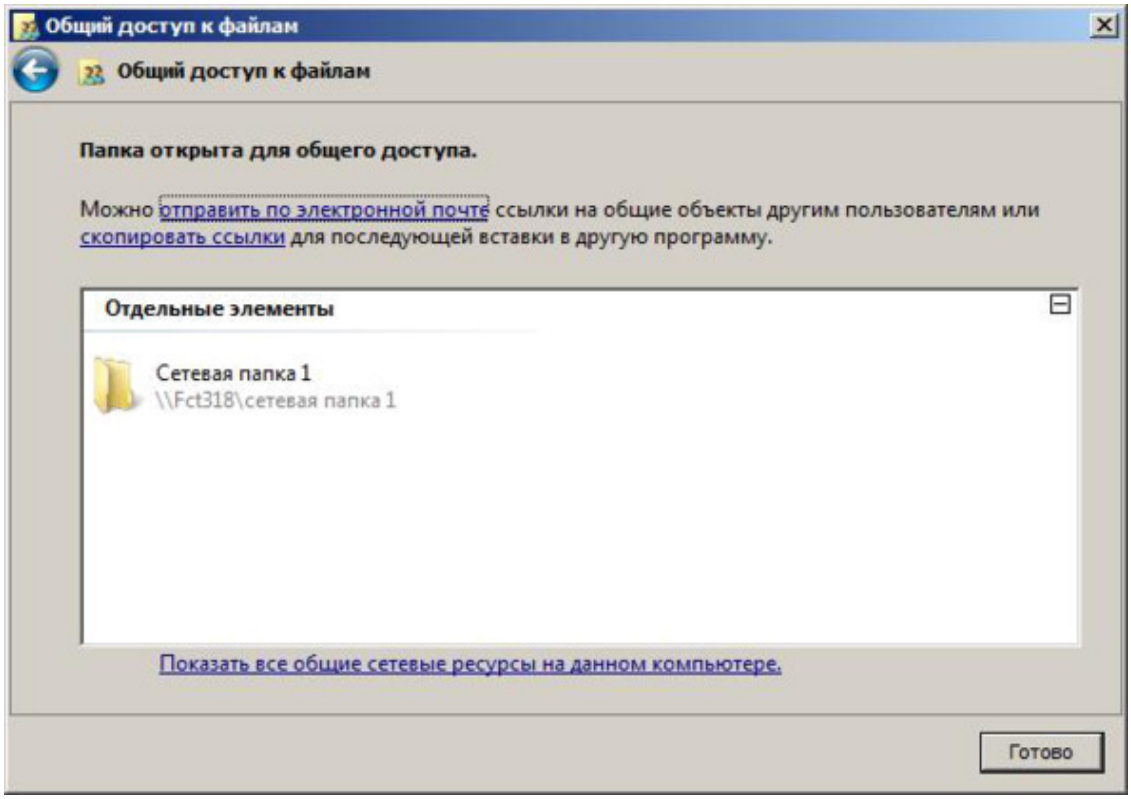


Рисунок 7 – Завершение настройки общего доступа

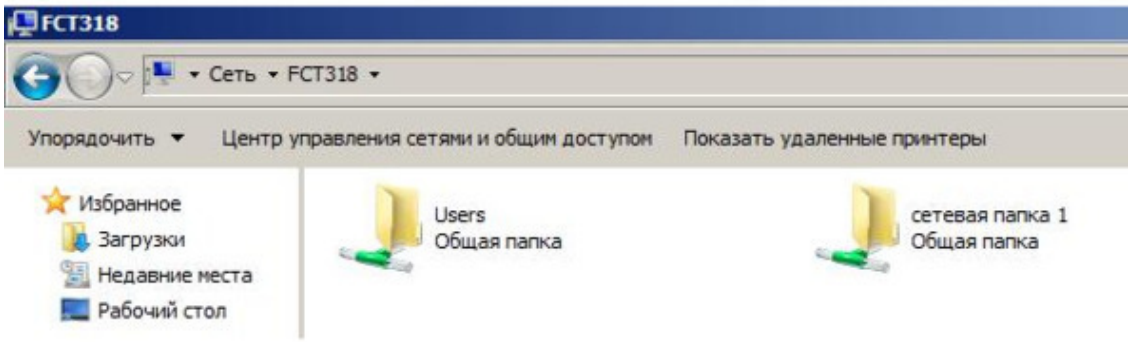


Рисунок 8 – Настроенная сетевая папка

На рисунках 9 и 10 показан текстовый файл «222222222223.txt» с набором цифр.

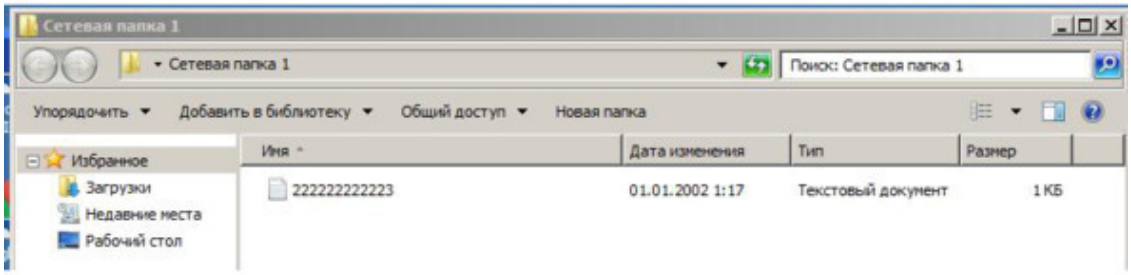


Рисунок 9 – Текстовый файл «222222222223.txt»

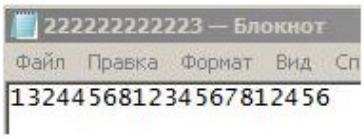


Рисунок 10 – Содержимое текстового файла «222222222223.txt»

Добавим в сетевую папку текстовый файл с некой информацией. Атакующий с запущенным Wireshark видит передающуюся информацию от PC1 к PC2 по протоколу SMB2 (рисунок 11). Проверив данный пакет, мы находим передаваемую в файле информацию (рисунок 12).

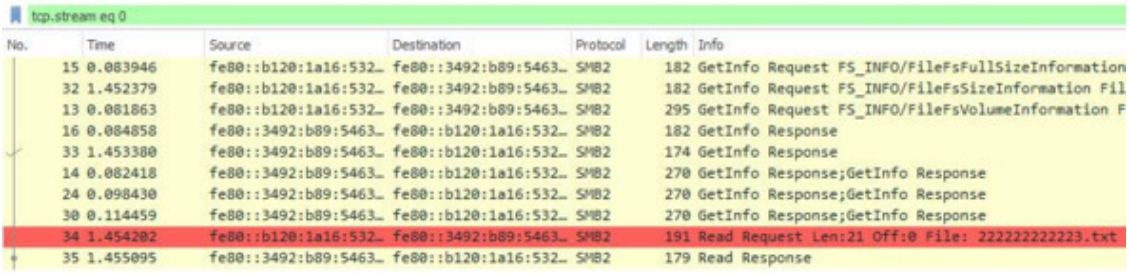


Рисунок 11 – Передающаяся информация от PC1 к PC2

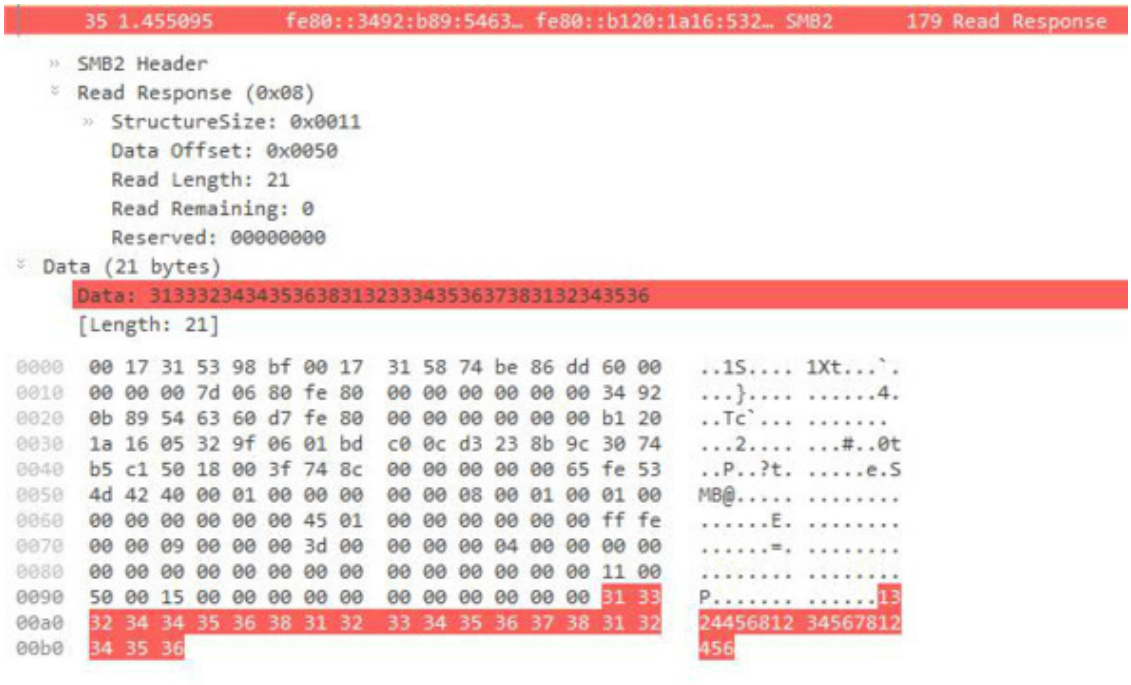


Рисунок 12 – Передаваемая в файле информация

Аналогично происходит и для файлов расширения. png и. rar. Найти нужные пакет можно по фильтру «smb2.write_length> 0». Полученную информацию можно восстановить из всех перехваченных пакетов любым HEX-редактором. Для этого кликнем ПКМ по найденному пакету с информацией и выберем «Export Packet Bytes…» Пример указан на рисунках 13 – 14. Аналогично выполняется и для. rar-файлов.

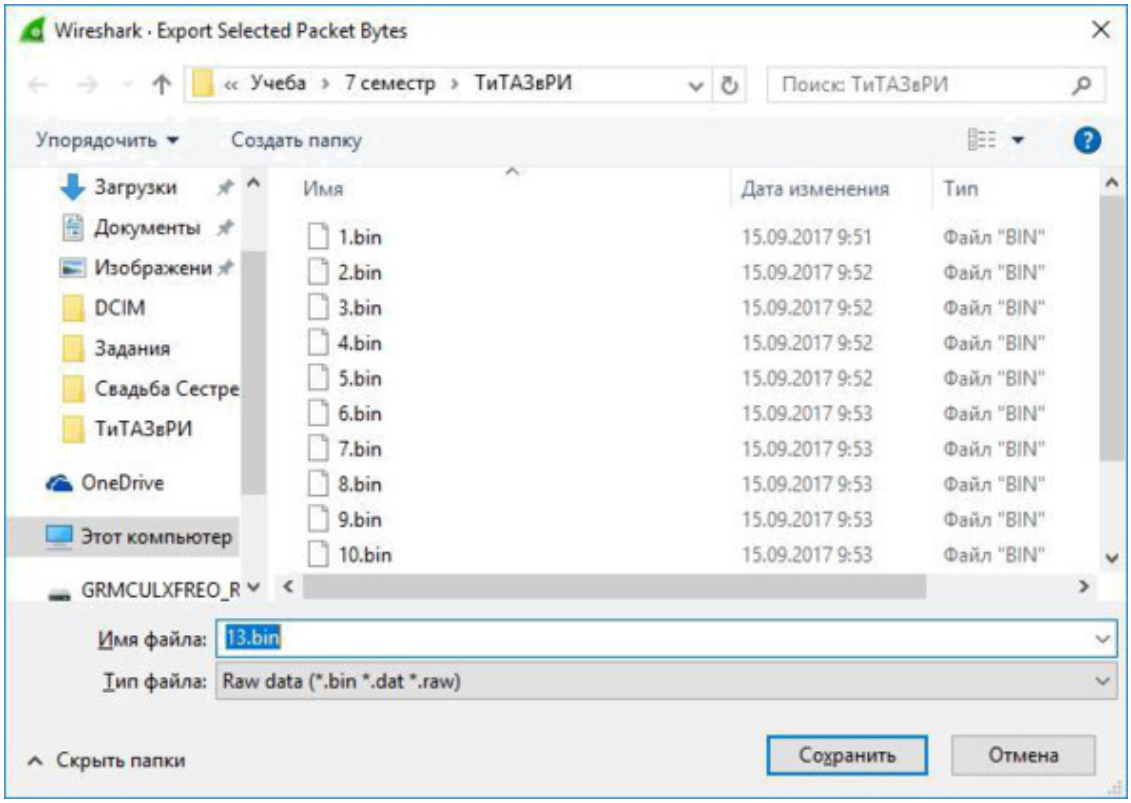


Рисунок 13 – Пример восстановления из всех перехваченных пакетов

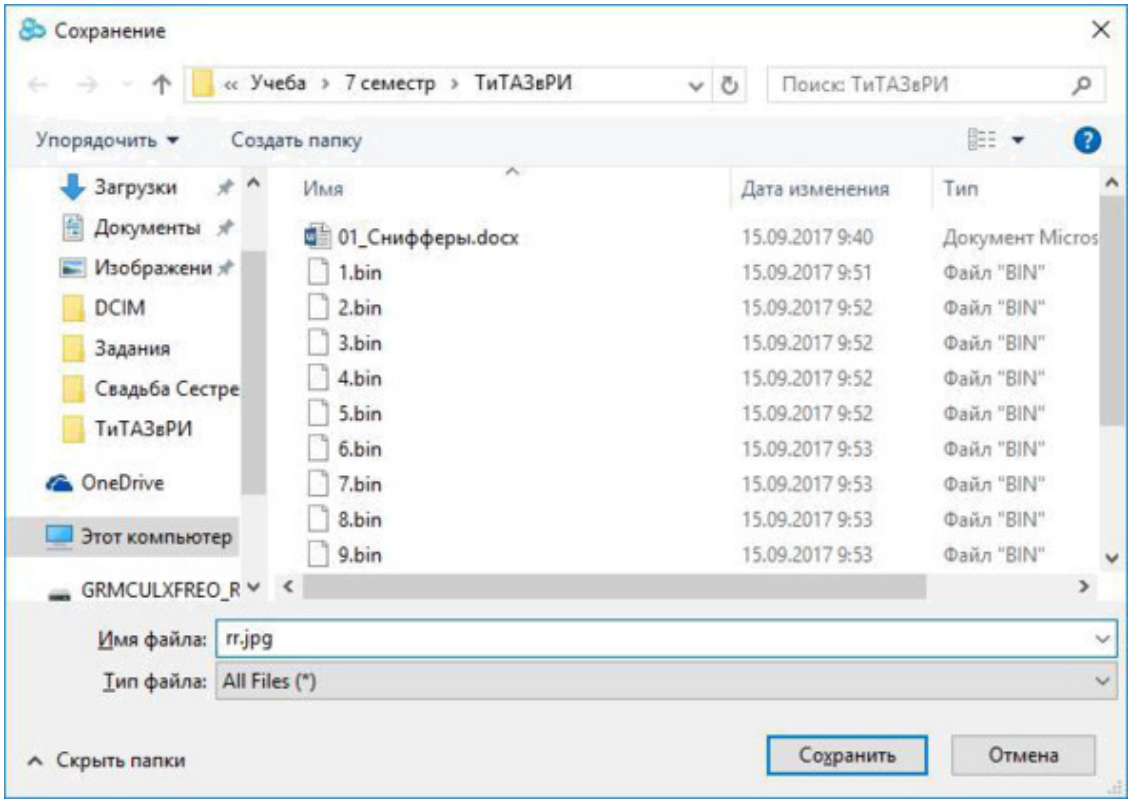


Рисунок 14 – Восстановленные данные

2.3 Перехват информации, используя протокол FTP

FTP (File Transfer Protocol) – протокол передачи файлов по сети. В отличие от TFTP, гарантирует передачу (либо выдачу ошибки) за счёт применения квитируемого протокола TCP. Типичное применение FTP-протокола – загрузка сайтов и других документов с частного устройства разработки на общедоступные сервера хостинга.

Для создания FTP-сервера требуется перейти в Пуск → Панель управления, выбираем «Программы и компоненты», выбираем «Включение или отключение компонентов Windows», в открывшемся окне выбираем «Расширяемость FTP», «Служба FTP» и «Консоль управления IIS». Жмем ОК и дожидаемся завершения процесса.

После этого переходим в Панель управления → Администрирование, выбираем «Диспетчер служб IIS». Нажимаем правую кнопку мыши и в выпадающем меню выбираем «Добавить FTP сайт». Указываем название сайта и его расположение. Нажимаем «Далее». В разделе «SSL» устанавливаем «Без SSL». Нажимаем «Далее». Проверку подлинности делаем обычную. Весь процесс настройки сайта показан на рисунках 15 – 19.

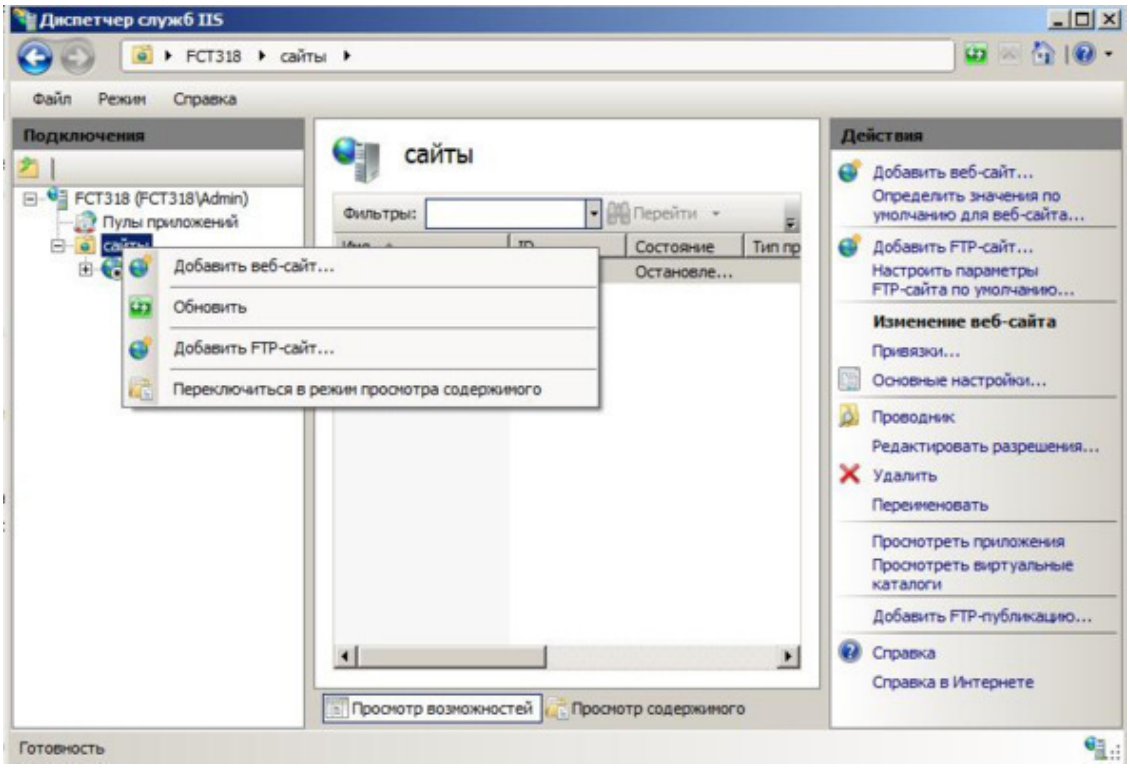


Рисунок 15 – Процесс настройки сайта

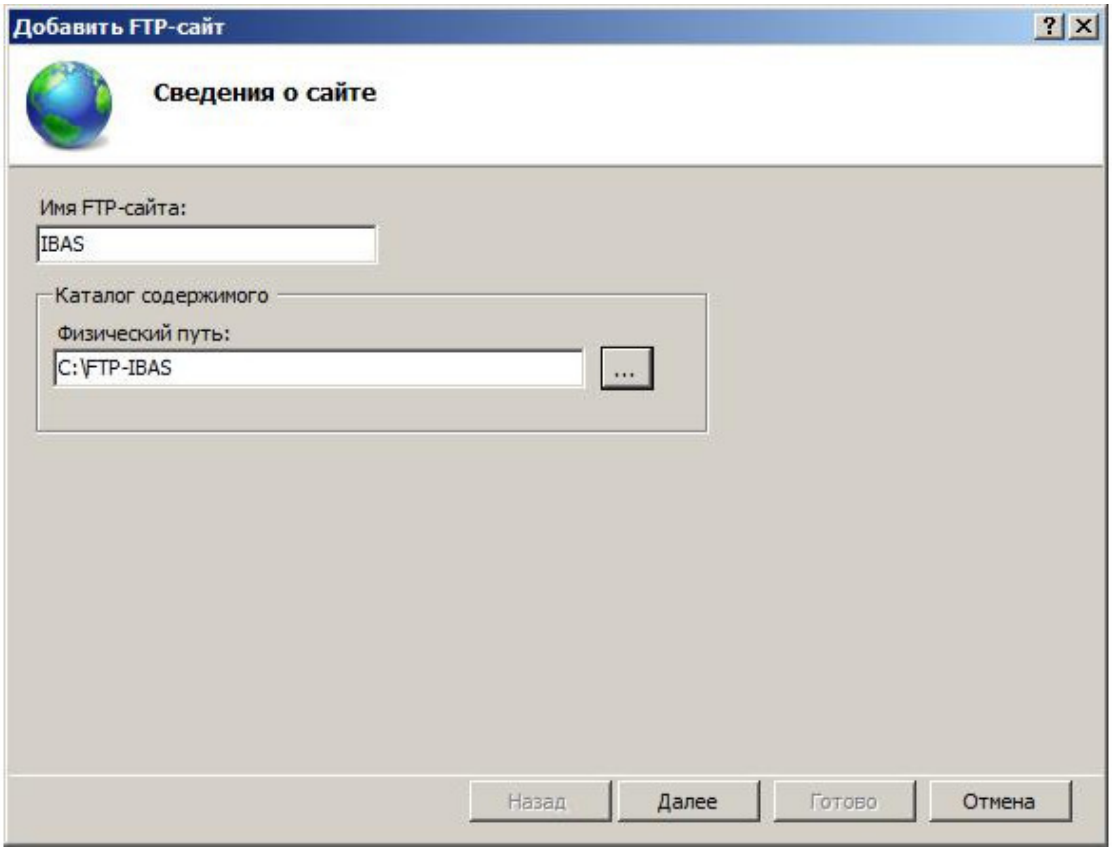


Рисунок 16 – Процесс настройки сайта

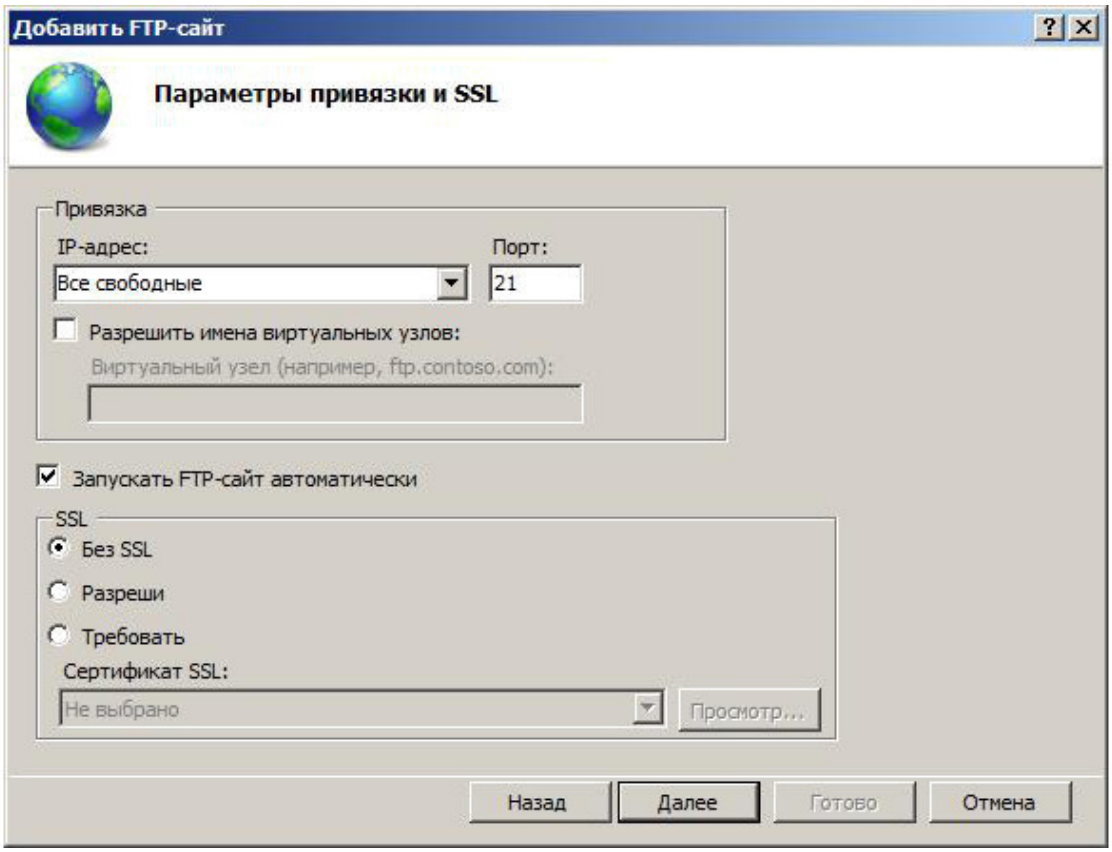


Рисунок 17 – Процесс настройки сайта

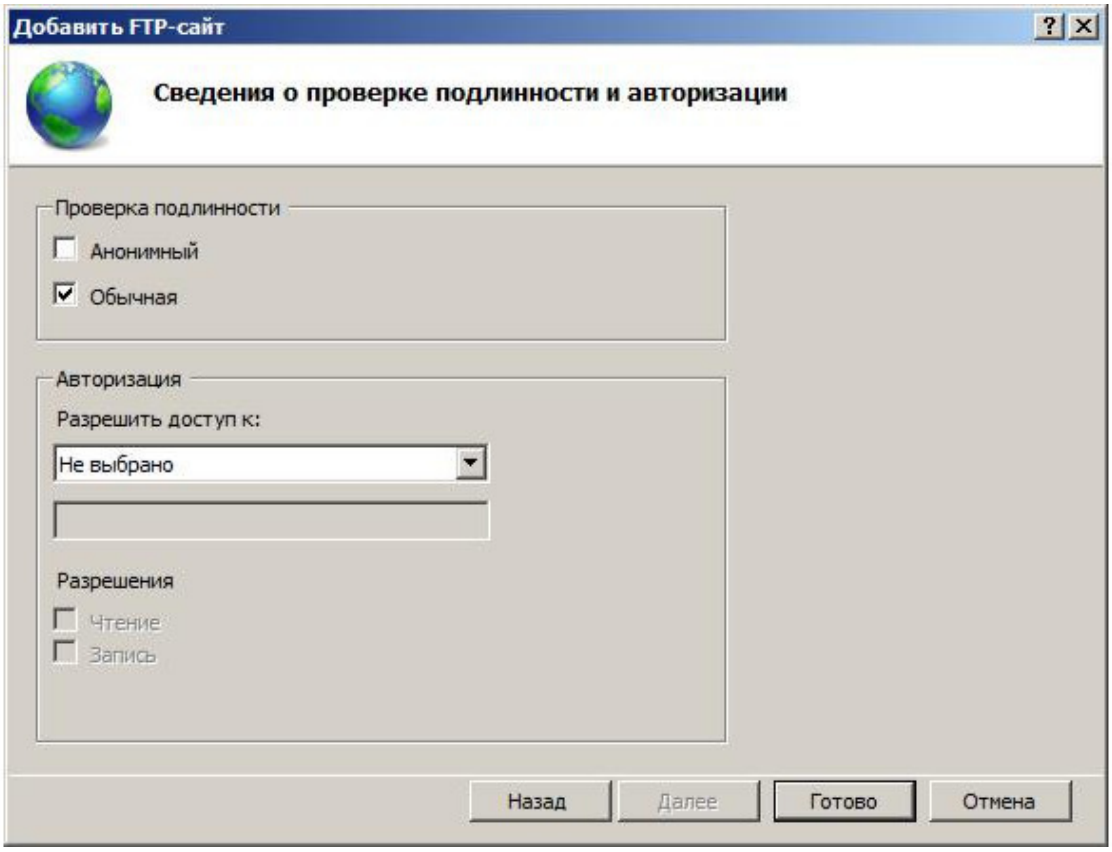


Рисунок 18 – Процесс настройки сайта

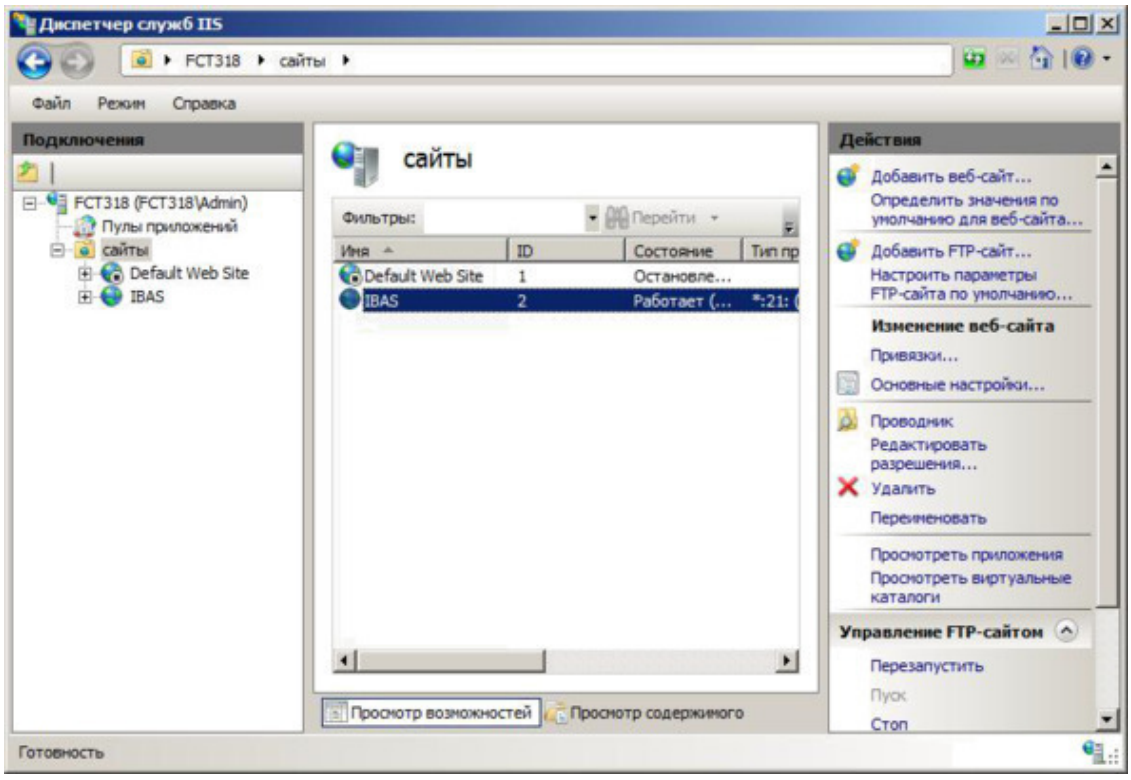


Рисунок 19 – Процесс настройки сайта

Сайт создан. Далее переходим в Панель управления → Брандмауэр → Дополнительные параметры → Правила для входящих соединений. Выбираем и активируем пункты FTP Server

Passive (чтобы можно было подключиться к FTP в пассивном режиме) и FTP сервер. Переходим в раздел «Правила для исходящих соединений» и активируем пункт «FTP Server».

Далее переходим Панель управления → Администрирование → Управление компьютером → Локальные пользователи → Группы → ПКМ → Создать группу. Указываем название группы и нажимаем «Создать». Далее переходим в Пользователи. ПКМ → Новый пользователь. Указываем имя пользователя, пароль (не менее 8 символов). Устанавливаем галочки напротив «Запретить смену пароля пользователем» и «Срок действия пароля неограничен». Далее выбираем пользователя, правый клик мыши, «Свойства», «Членство в группах». Нажимаем «Добавить» и выбираем группу «FTP», нажимаем «ОК».

Переходим в каталог, который мы указали для FTP сервера. ПКМ → Свойства → Безопасность → Изменить. Далее «Добавить», указываем название группы и «ОК». Устанавливаем разрешения «Разрешить все».

Переходим в Панель управления → Администрирование → Диспетчер служб IIS и выбираем наш FTP. Переходим в «Правила авторизации FTP». Выбираем «Добавить разрешающее правило» и указываем нашу группу «FTP». Ставим галочки напротив «Чтение» и «Запись». Нажимаем «ОК». Устанавливаем максимальный размер лога или отключаем вообще (по желанию).

Данные настройки продемонстрированы на рисунках 20 – 27.

Рисунок 20 – Процесс настройки FTP

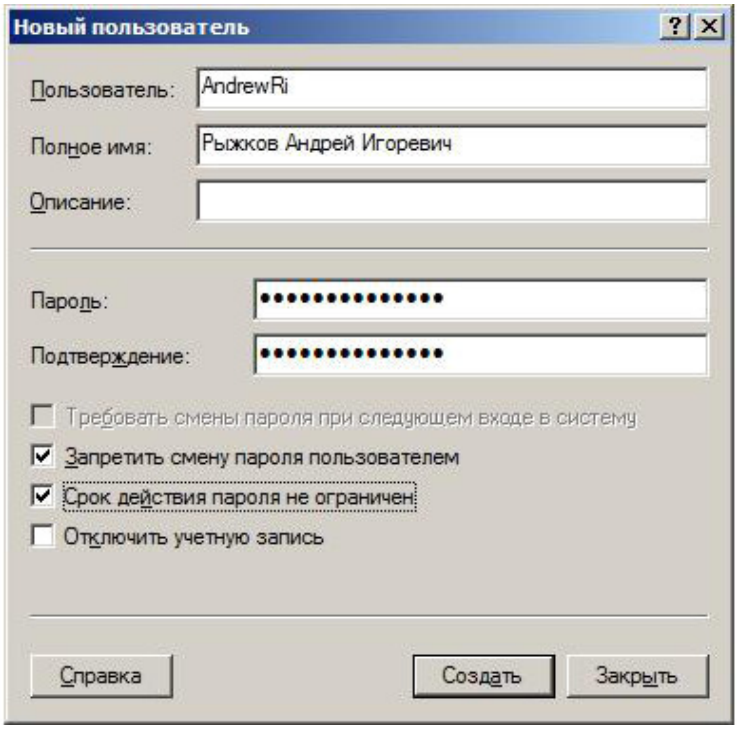


Рисунок 21 – Процесс настройки FTP

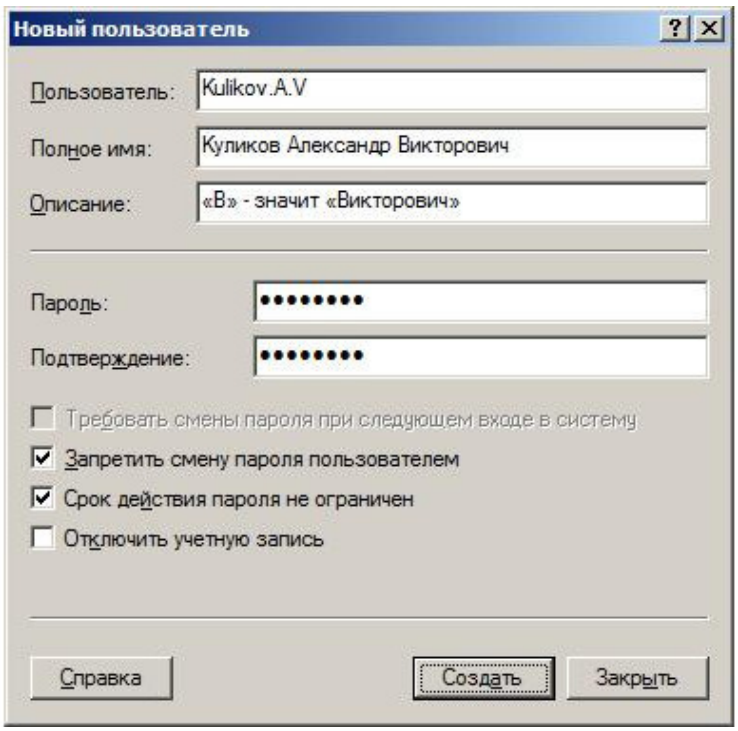


Рисунок 22 – Процесс настройки FTP

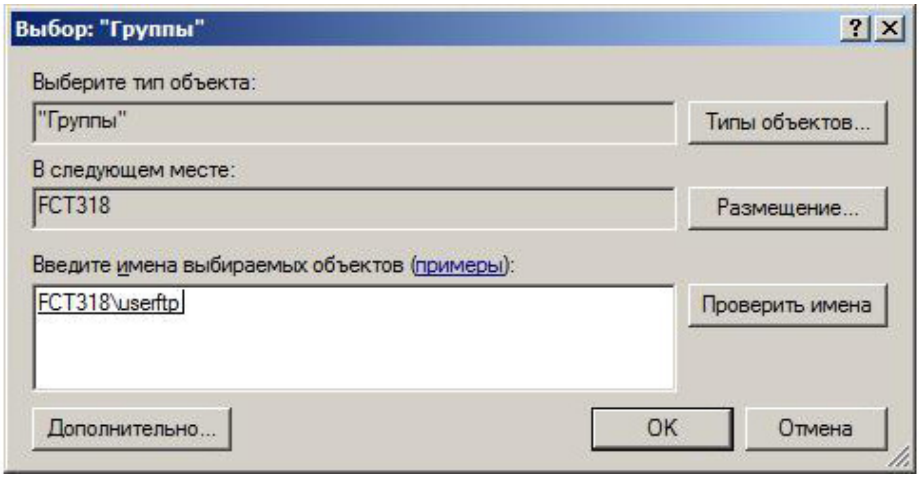


Рисунок 23 – Процесс настройки FTP

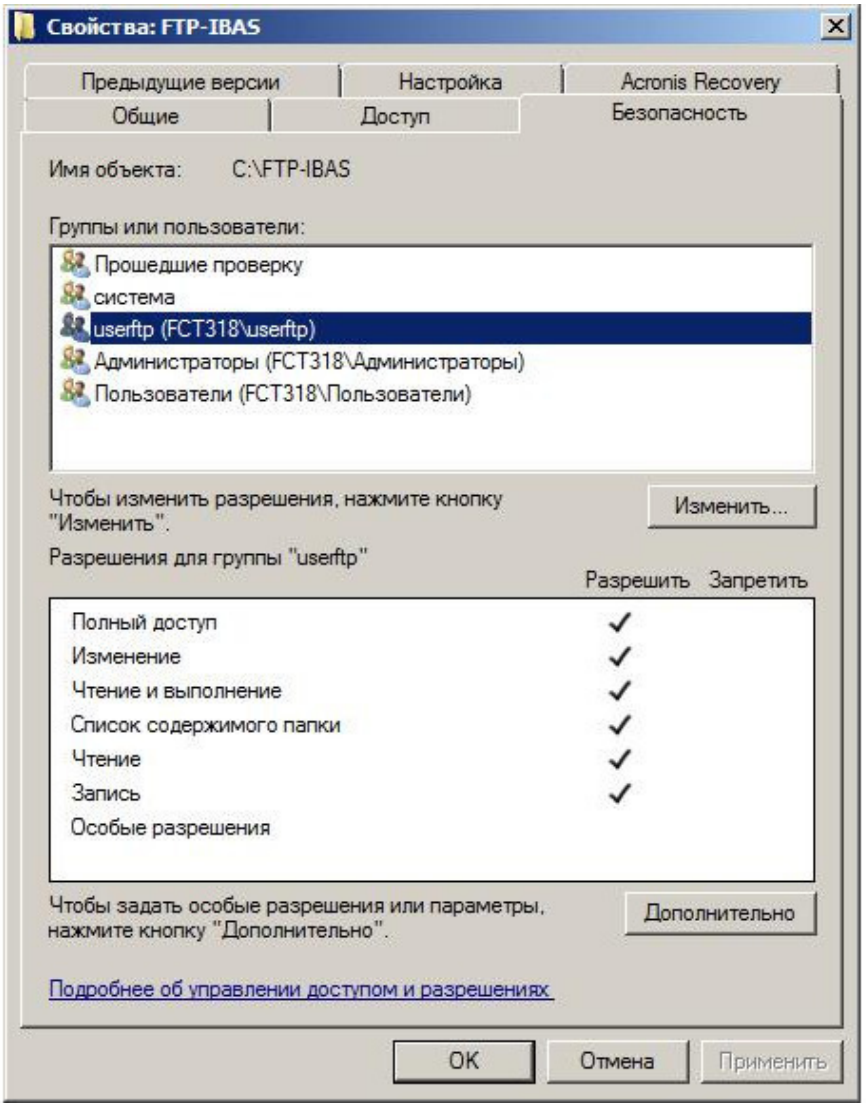


Рисунок 24 – Процесс настройки FTP

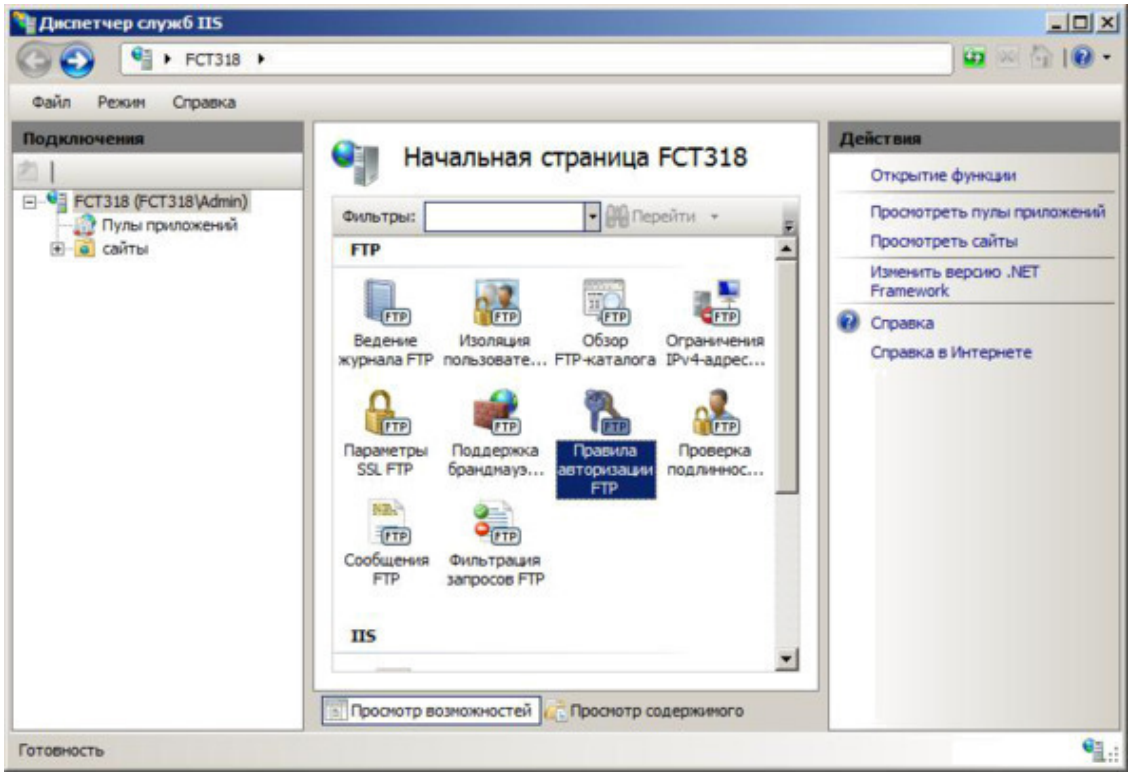


Рисунок 25 – Процесс настройки FTP

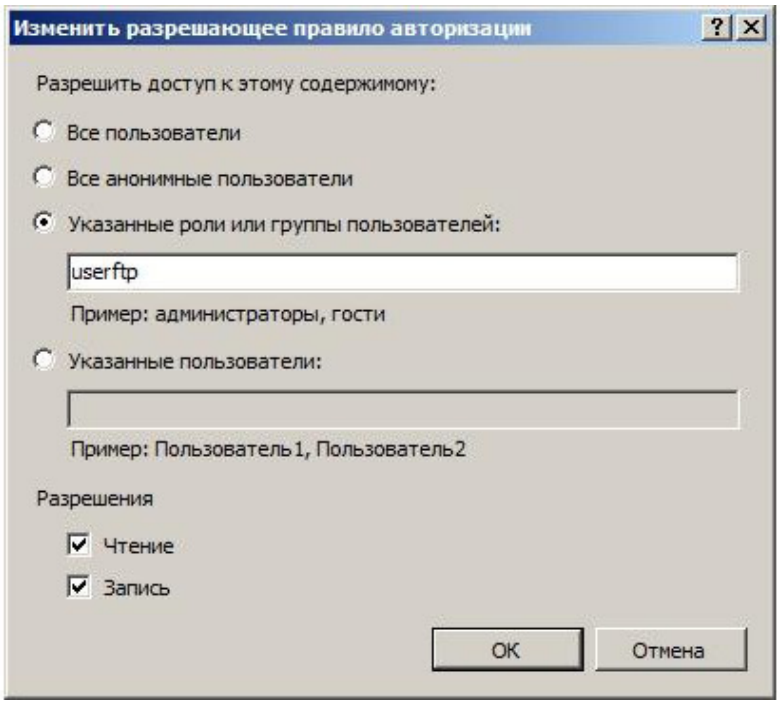


Рисунок 26 – Процесс настройки FTP

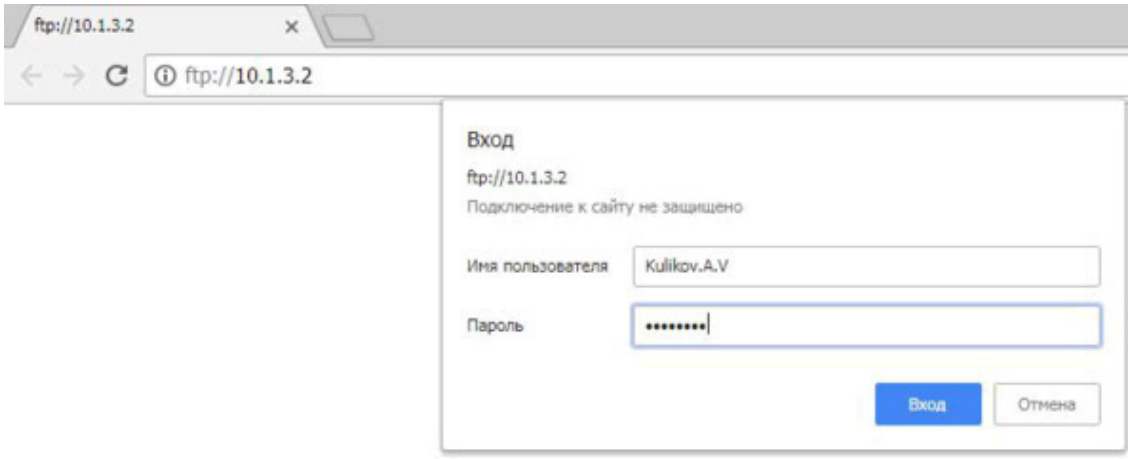


Рисунок 27 – Процесс настройки FTP

Сервер установлен. В папку помещаем файлы, которые будут хранится на этом сервере и к которому будут иметь доступ авторизированные пользователи. Подключится к серверу можно с помощью любого FTP-клиента (например, с помощью FileZilla) или непосредственно с помощью браузера, введя в адресную строку IPv4-адрес нашего FTP-сервера (который соответствует IPv4-адресу PC1).

В браузере, в адресную строку вводим IPv4-адрес нашего FTP-сервера. Он запросит логин и пароль. Вводим их и попадаем на сервер с хранящейся там информацией. Данные, используемые для входа можно также увидеть на рисунке 27, а на рисунке 28 показаны файлы, находящиеся на сервере.

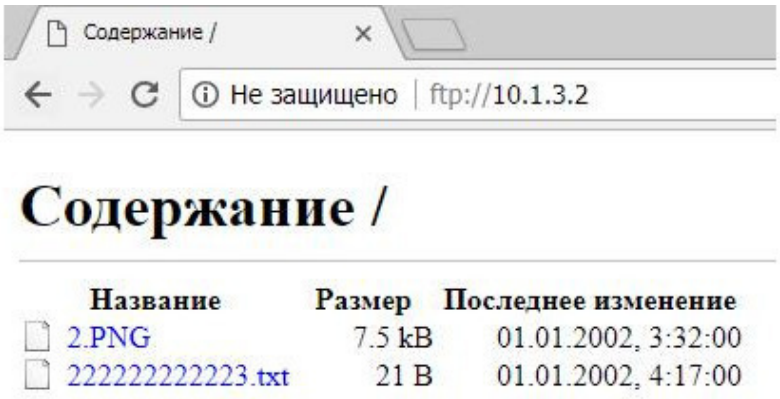
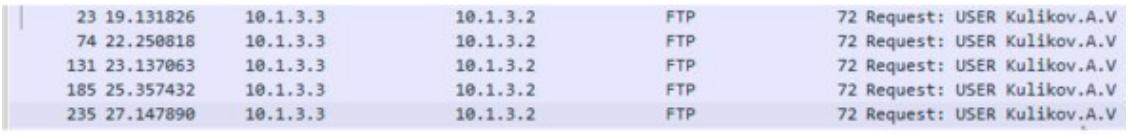


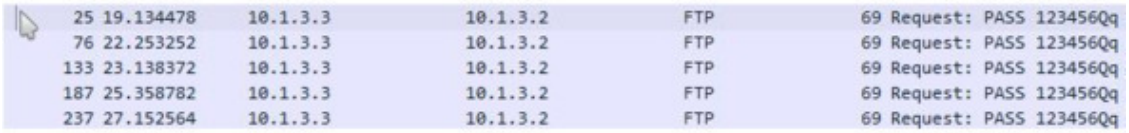
Рисунок 28 – Информация на FTP-сервере

Атакующий компьютер с Wireshark находит нужные пакеты по протоколу FTP. В них указаны наши логин и пароль (рисунки 29- 30).



23	19.131826	10.1.3.3	10.1.3.2	FTP	72 Request: USER Kulikov.A.V
74	22.250818	10.1.3.3	10.1.3.2	FTP	72 Request: USER Kulikov.A.V
131	23.137063	10.1.3.3	10.1.3.2	FTP	72 Request: USER Kulikov.A.V
185	25.357432	10.1.3.3	10.1.3.2	FTP	72 Request: USER Kulikov.A.V
235	27.147890	10.1.3.3	10.1.3.2	FTP	72 Request: USER Kulikov.A.V

Рисунок 29 – Пакеты с логином и паролем



25	19.134478	10.1.3.3	10.1.3.2	FTP	69 Request: PASS 123456Qq
76	22.253252	10.1.3.3	10.1.3.2	FTP	69 Request: PASS 123456Qq
133	23.138372	10.1.3.3	10.1.3.2	FTP	69 Request: PASS 123456Qq
187	25.358782	10.1.3.3	10.1.3.2	FTP	69 Request: PASS 123456Qq
237	27.152564	10.1.3.3	10.1.3.2	FTP	69 Request: PASS 123456Qq

Рисунок 30 – Пакеты с логином и паролем

2.4 Перехват информации, с использованием протокола Telnet

Telnet – сетевой протокол для реализации текстового интерфейса по сети. Вся информация, отображаемая и вводимая на консольный интерфейс, передается по сети в виде открытого текста.

Для установки Telnet требуется открыть Панель управления. По умолчанию, Telnet не будет установлен на Windows 7. Надо его активировать вручную, чтобы использовать. Вы можете сделать это через Панель управления, к которой можете получить доступ через меню Пуск. После открыть «Программы и Компоненты» и «Включение или отключение компонентов Windows».

В компонентах Windows следует выбрать Telnet-сервер (рисунок 31).

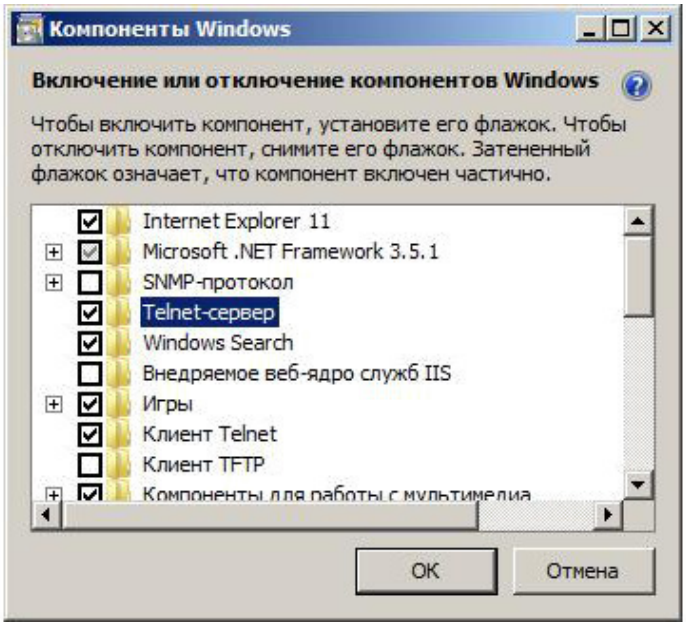


Рисунок 31 – Выбор Telnet-сервера

Дальше запускаем службы Windows. В командной строке вводим «net start tlntsvr» (рисунок 32).

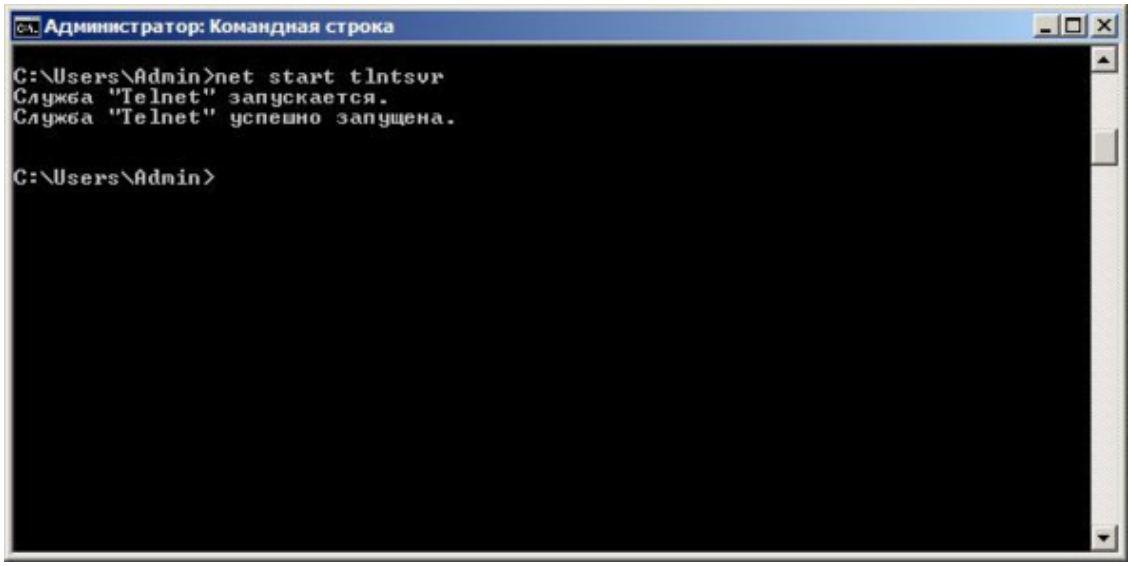


Рисунок 32 – Команда в командной строке

Теперь к компьютеру можно будет подключатся через протокол Telnet, используя соответствующие программы, например, PuTTY. В качестве логина и пароля используем логин и пароль пользователя, который есть на компьютере (рисунки 33 – 34).

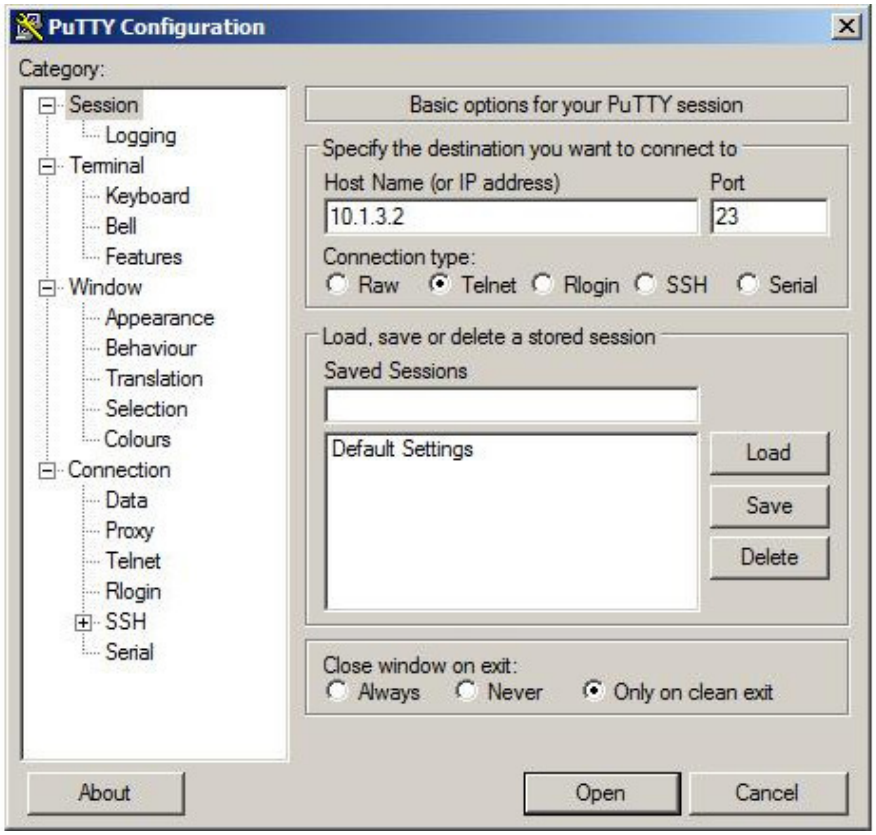


Рисунок 33 – Подключение через протокол Telnet

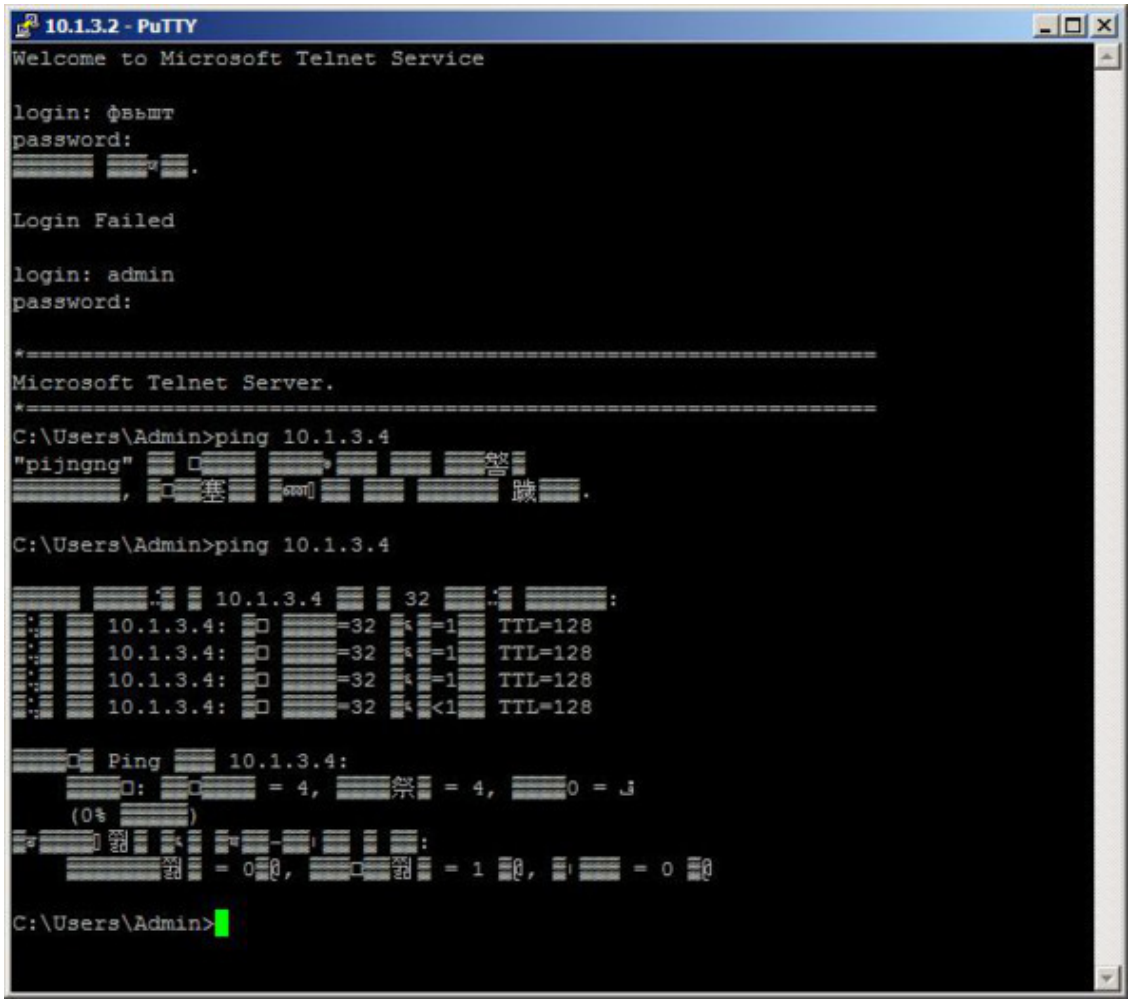


Рисунок 34 – Данные, полученные при подключении

Атакующий компьютер с Wireshark находит нужные пакеты по протоколу TCP. Выберем один из перехваченных пакетов, ПКМ → Follow → TCP Stream. Теперь мы видим все, что было в консольном интерфейсе PuTTY (рисунки 35 – 36).

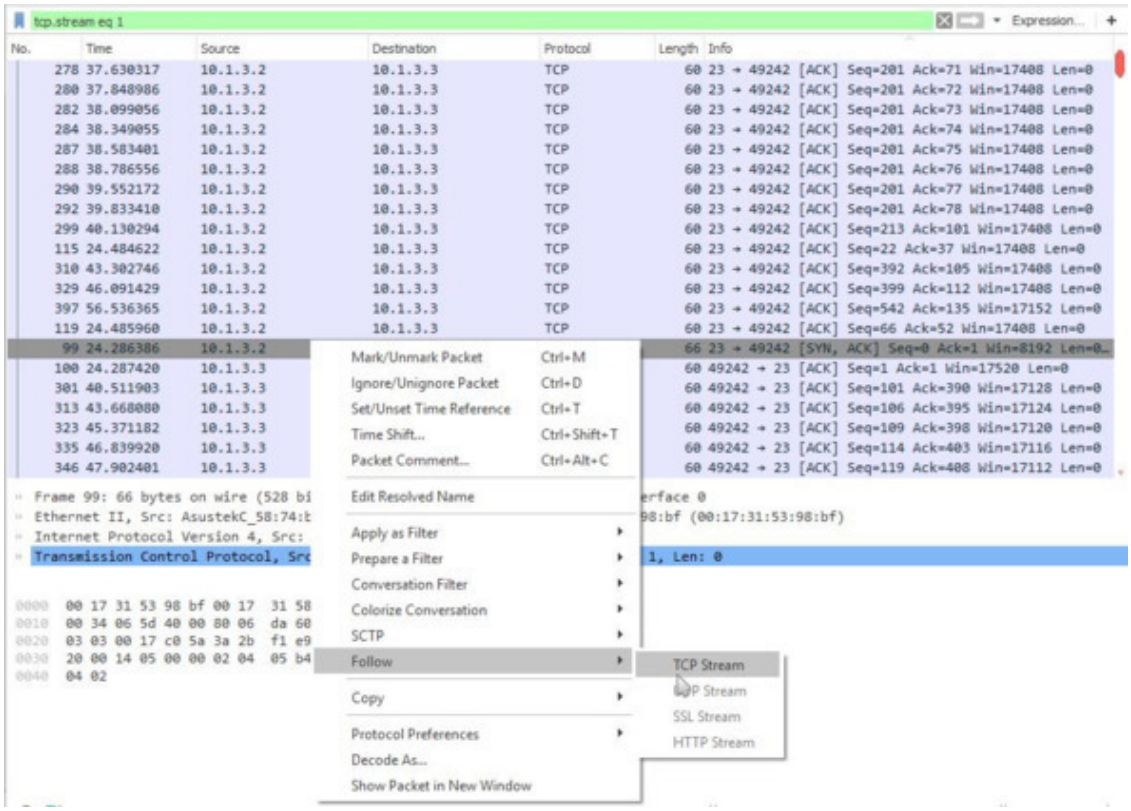


Рисунок 35 – Перехваченные пакеты

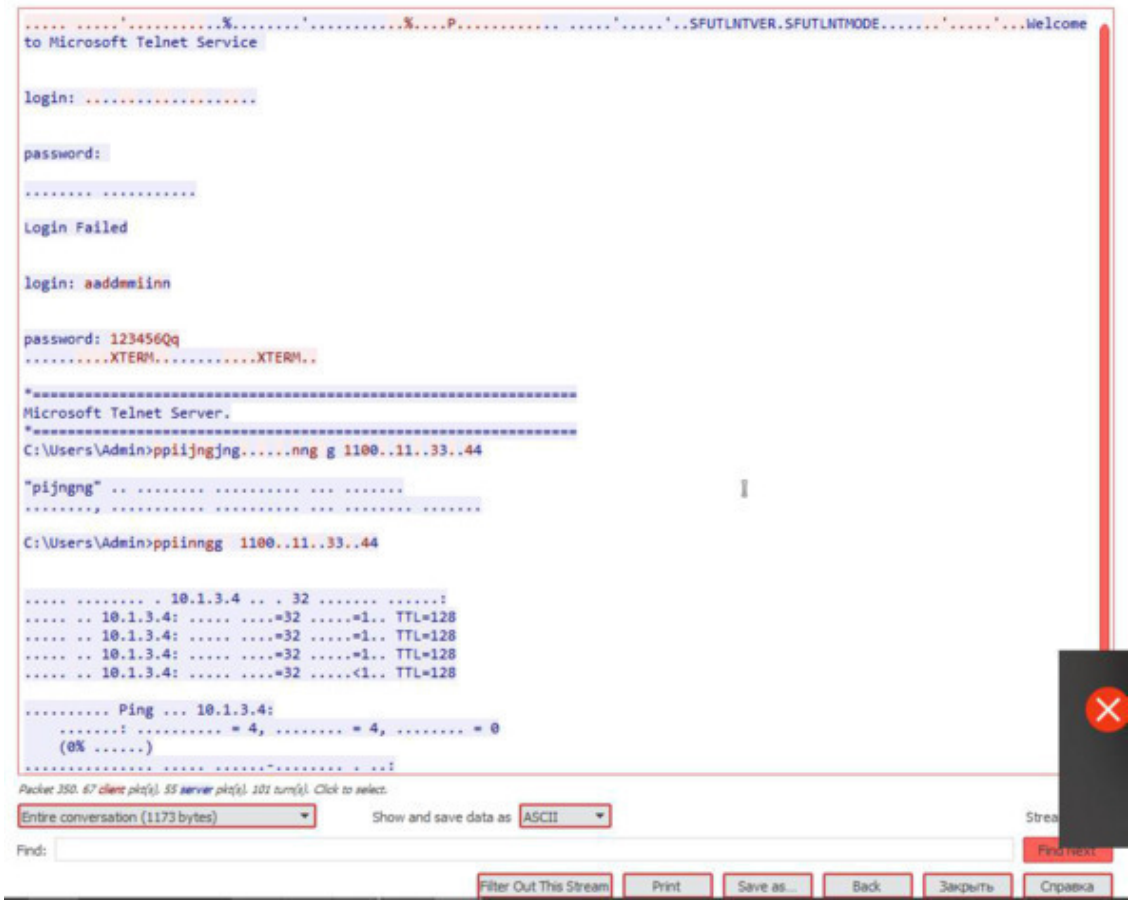


Рисунок 36 – Перехваченные пакеты

2.5 Перехват информации, используя протокол HTTP

HTTP (HyperText Transfer Protocol – «протокол передачи гипертекста») – протокол прикладного уровня передачи различных мультимедийных данных. Главное отличие от аналогичного протокола HTTPS – отсутствие шифрования, из-за чего вся информация, отображаемая и вводимая на консольный интерфейс, передается по сети в виде открытого текста.

Откроем сайт, работающем на протоколе HTTP, например, http://olymp.knastu.ru. Вводим любой логин/пароль (рисунок 37).

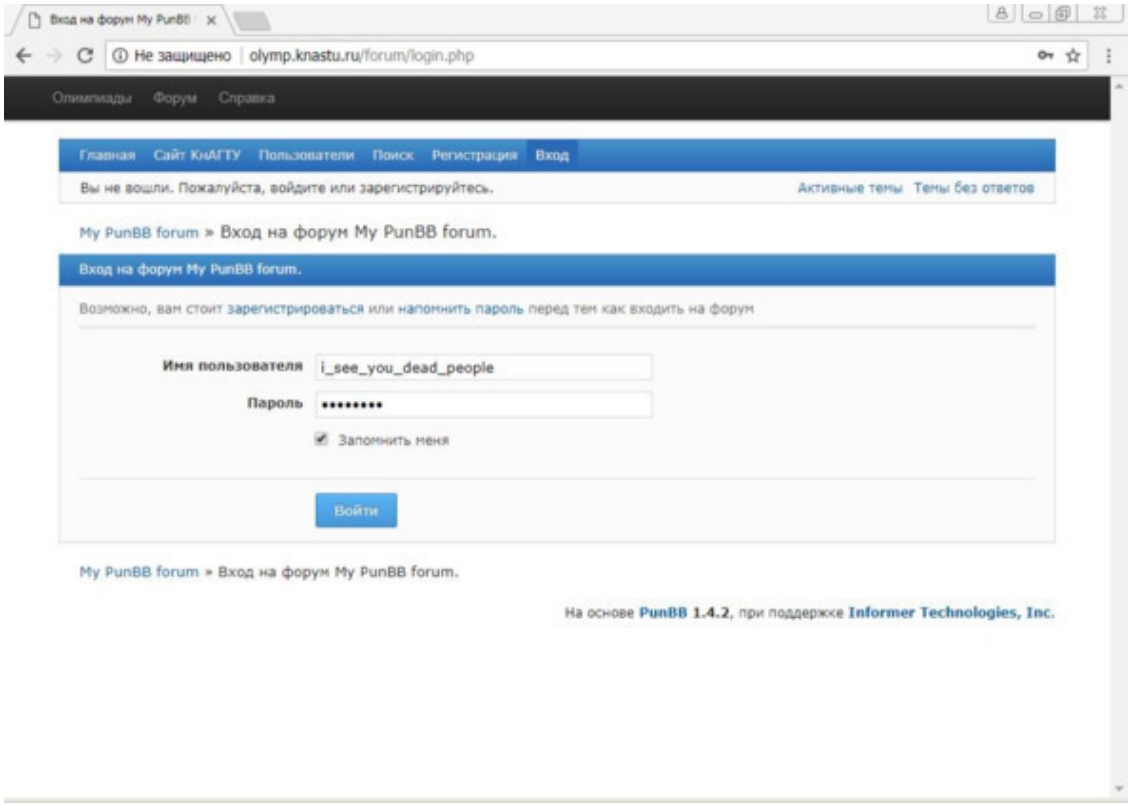


Рисунок 37 – Ввод логина и пароля

Атакующий компьютер с Wireshark находит нужные пакеты по протоколу HTTP. Анализируем их. Видим пару логин/пароль, которая вводила жертва.

3. Сетевые атаки
3.1 MAC-флудинг

Флудинг MAC – возможность неправомерного просмотра трафика в сети. Все MAC адреса хранятся на коммутаторах. Если переполнить сеть большим количеством поддельных MAC, то память коммутатора переполняется, и тогда коммутатор «превращается» в концентратор.

Для проверки уязвимости соберем лабораторный стенд по топологии, представленный на рисунке 38. На атакующем компьютере с помощью виртуальной машины был развернут дистрибутив GNU/Linux «Kali Linux». По умолчанию на нем установлена утилита «macof», совершающая MAC-флудинг на коммутатор.

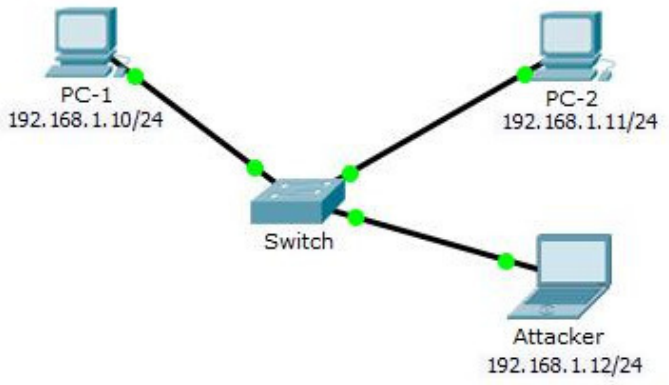


Рисунок 38 – Схема лабораторного стенда

На атакующем компьютере с Kali Linux через терминал запускаем утилиту командой «macof». Через несколько минут после начала флудинга таблица маршрутизации коммутатора переполняется и коммутатор становится концентратором, который передает пакеты всем подключенным узлам в сети.

После этого подключаем к коммутатору две жертвы: PC1 и PC2, между котороми будет проходить Echo-запрос с помощью команды «ping адрес».

В нашем случае IPv4-адрес атакующего имел вид 10.10.1.1, IPv4-адреса жертв: 10.10.1.3 и 10.10.1.6 соответственно. После произведенного MAC-флудинга атакующий компьютер с помощью Wireshark смог перехватить пакеты, предназначенные для других узлов (рисунок 39).

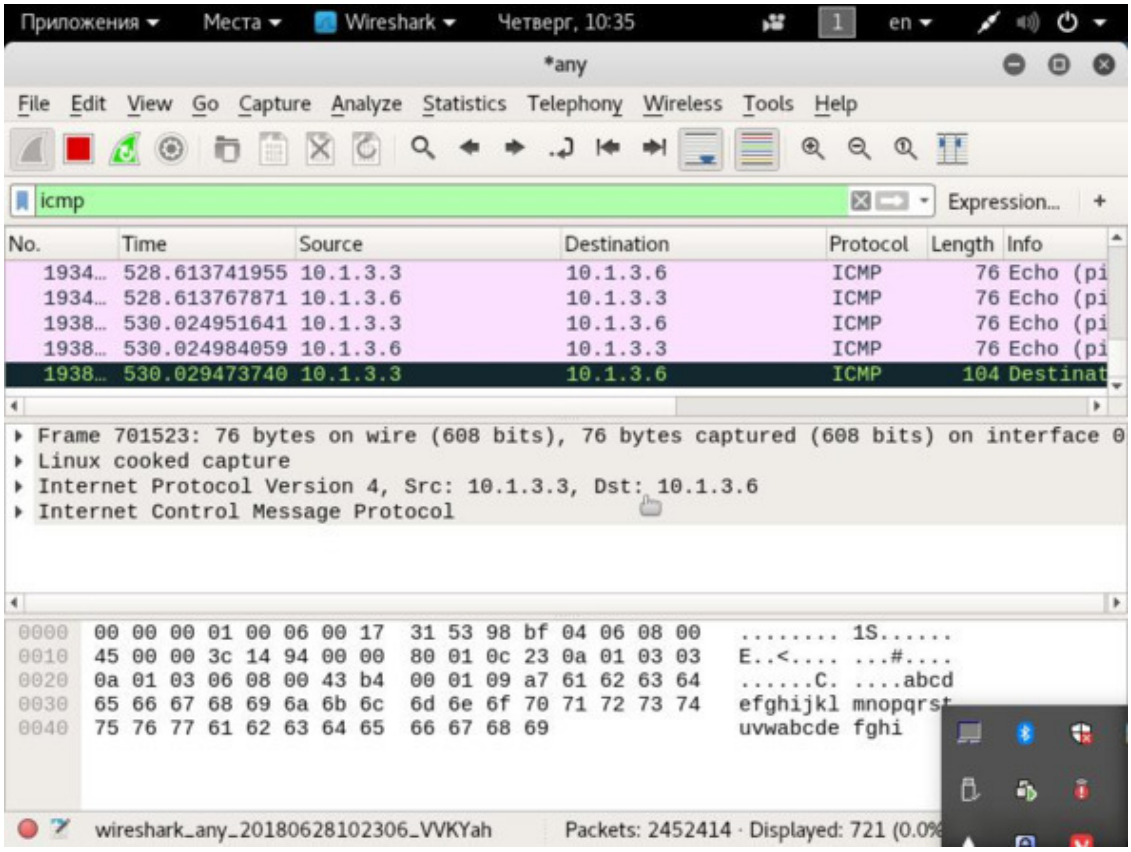


Рисунок 39 – Перехват пакетов

3.2 ARP-спуфинг

Классический пример атак типа «человек посредине». Протокол ARP является уязвимым – отсутствует проверка подлинности ARP-запросов и ARP-ответов. А

Для проверки уязвимости соберем лабораторный стенд по топологии, представленный на рисунке 40. Для ARP-спуфинга воспользуемся программой Cain & Abel.

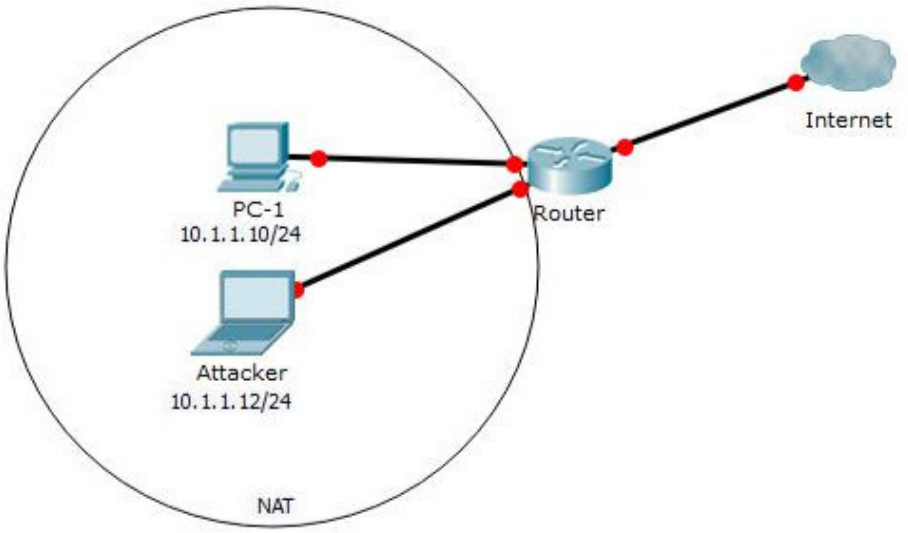


Рисунок 40 – Лабораторный стенд

В программе (рисунок 41) активируем кнопку «Start/Stop Sniffer».

Рисунок 41 – Активация программы

Перейдем во вкладку Sniffer. Нажмем кнопку «Add to list» (изображение плюса) и укажем диапазон нужных IP-адресов, которые находятся в сети. После этого в списке будут видны IPv4-адрес маршрутизатора (10.10.1.254) и IPv4-адрес жертвы (10.10.1.13). Это показано на рисунке 42.

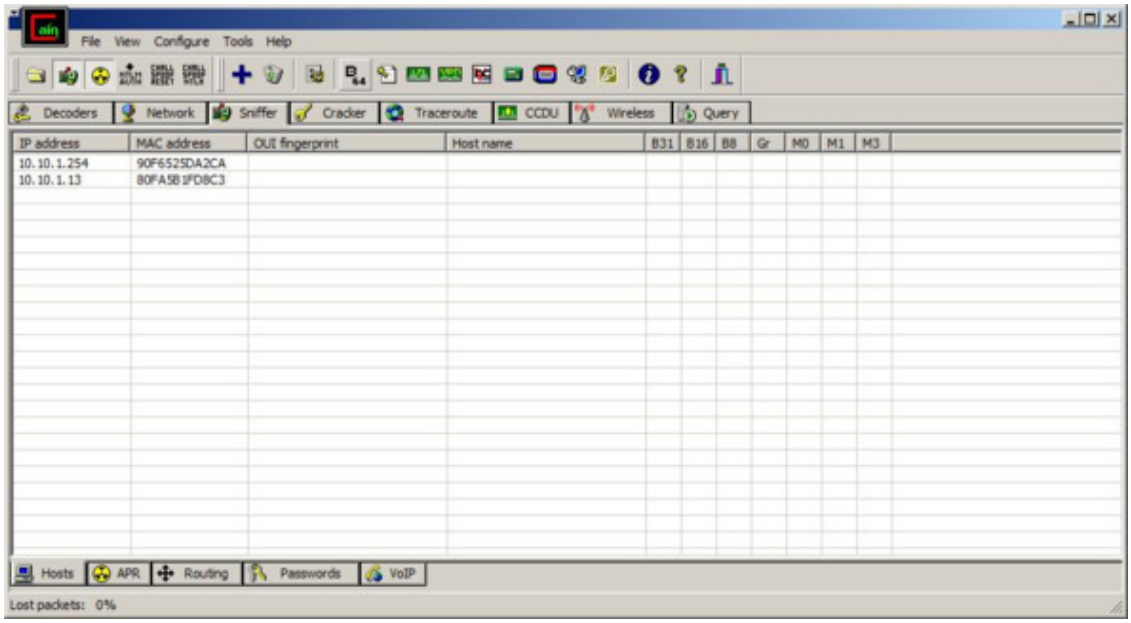


Рисунок 42 – IPv4-адрес маршрутизатора и жертвы

Перейдем во вкладку ARP. Нажмем кнопку «New ARP Poison Routing» (изображение плюса). В нем необходимо выбрать IPv4-адрес жертвы (рисунок 43). Активируем кнопку «Start/Stop ARP».

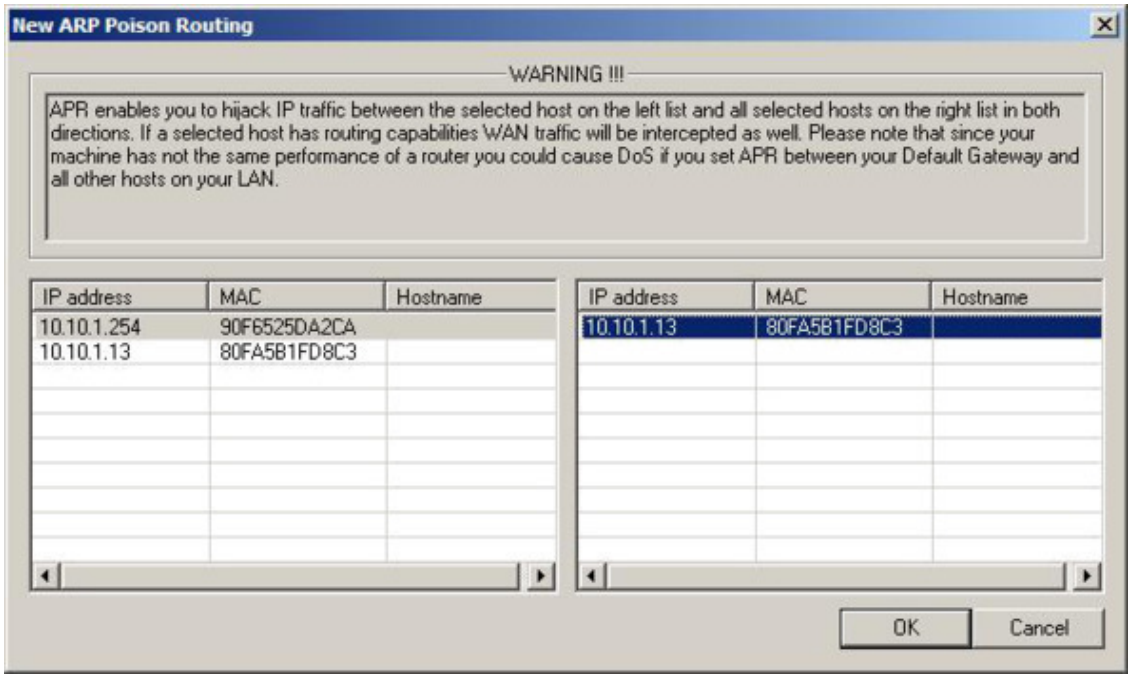


Рисунок 43 – Вкладка ARP

На компьютере жертвы откроем сайт, работающем на протоколе HTTP, например, http://olymp.knastu.ru. Вводим любой логин/пароль (рисунок 44). Атакующий получает логин/пароль от жертвы (рисунок 45).

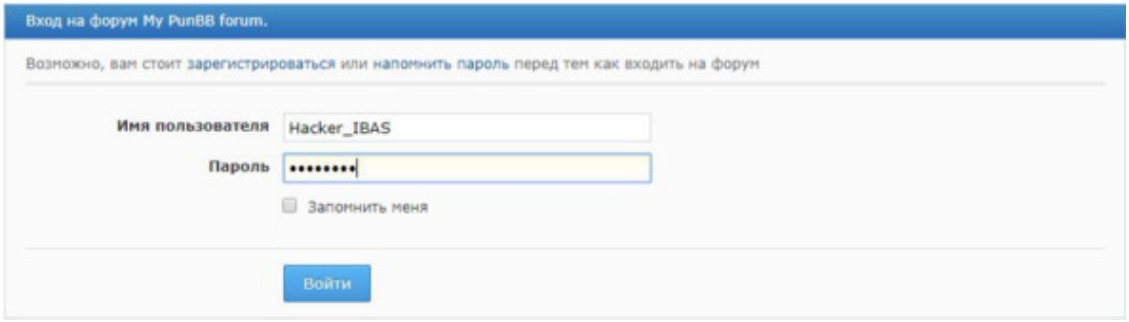


Рисунок 44 – Ввод логина и пароля

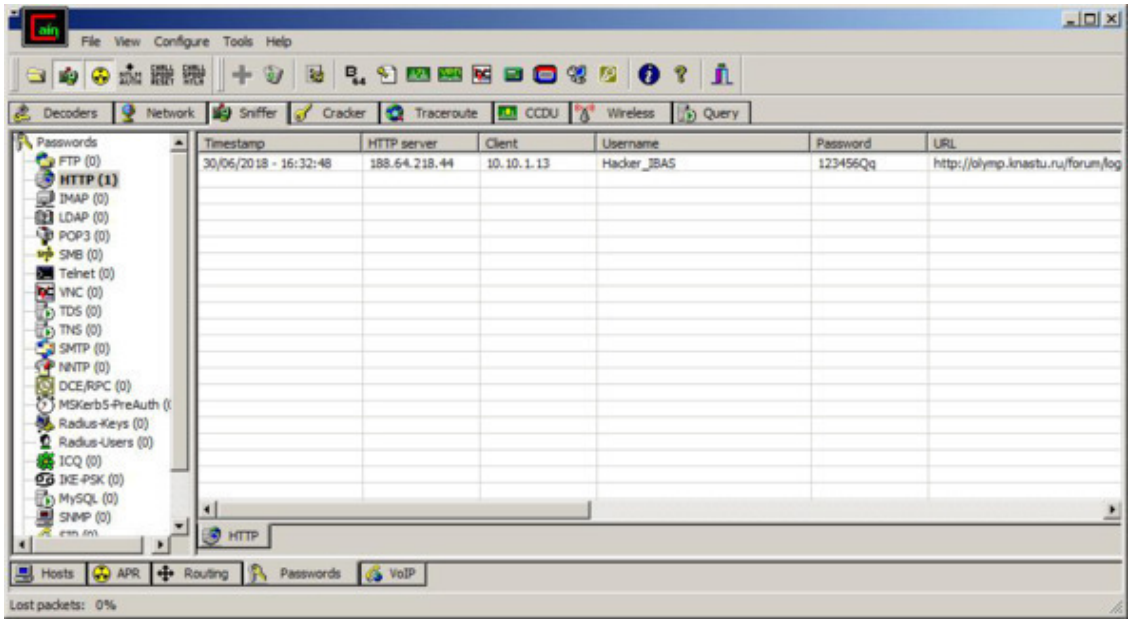


Рисунок 45 – Получение логина и пароля жертвы

2 Применение сетевых атак

2.1 Истощение ресурсов DHCP и подмена DHCP-сервера

Идея состоит в получении пакетов клиента для конфигурации сетевых параметров и подмены шлюза. Таким образом неавторизованный DHCP-сервер может прослушивать весь трафик.

Для проверки уязвимости соберем лабораторный стенд по топологии, представленный на рисунке 46.

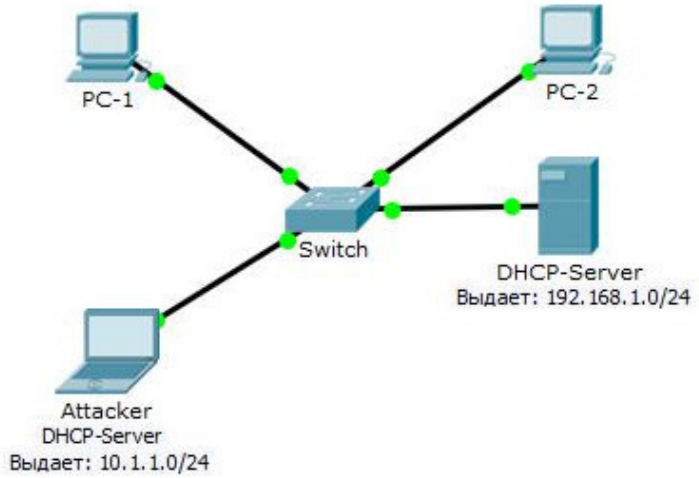


Рисунок 46 – Схема лабораторного стенда

На атакующем компьютере с помощью виртуальной машины был развернут дистрибутив GNU/Linux «Kali Linux». Атаку будем выполнять при помощи утилиты «dhcpstarv». Прежде эту программу необходимо установить при помощи команды в терминале – apt-get install dhcpstarv. Для запуска утилиты, необходимо ввести команду – dhcpstarv —i eth0 (где eth0 – порт для выхода в сеть, его узнать можно с помощью команды ifconfig). Данная программа записывает на себя все доступные адреса, поставляемые DHCP сервером. Как результат – сервер не может выполнять свою функцию. На рисунке 47 показана работа программы, а на рисунке 48 продемонстрировано, как заполняются все доступные IPv4-адреса в DHCP-сервере.

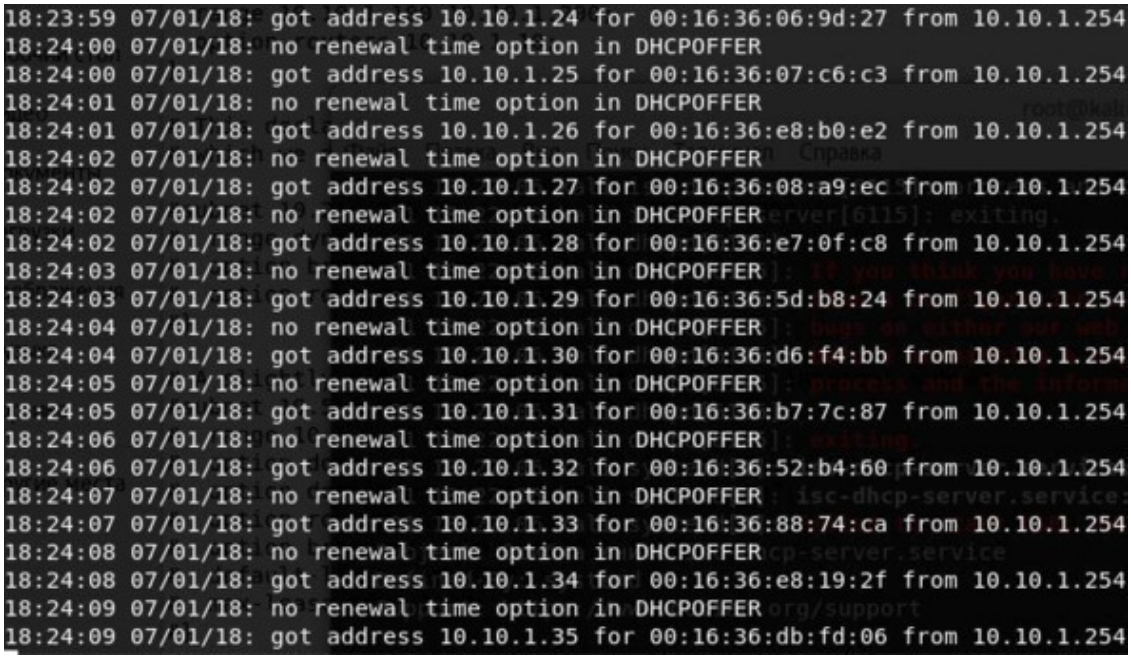


Рисунок 47 – Работа программы

15	Unknown	00-16-36-39-92-DC	10.10.1.23	01:59:35
16	Unknown	00-16-36-06-9D-27	10.10.1.24	01:59:36
17	Unknown	00-16-36-07-C6-C3	10.10.1.25	01:59:37
18	Unknown	00-16-36-E8-B0-E2	10.10.1.26	01:59:38
19	Unknown	00-16-36-08-A9-EC	10.10.1.27	01:59:39
20	Unknown	00-16-36-E7-0F-C8	10.10.1.28	01:59:40
21	Unknown	00-16-36-5D-B8-24	10.10.1.29	01:59:41
22	Unknown	00-16-36-D6-F4-BB	10.10.1.30	01:59:42
23	Unknown	00-16-36-B7-7C-87	10.10.1.31	01:59:43
24	Unknown	00-16-36-52-B4-60	10.10.1.32	01:59:44
25	Unknown	00-16-36-88-74-CA	10.10.1.33	01:59:45
26	Unknown	00-16-36-E8-19-2F	10.10.1.34	01:59:46
27	Unknown	00-16-36-DB-FD-06	10.10.1.35	01:59:47
28	Unknown	00-16-36-96-B3-E6	10.10.1.36	01:59:48
29	Unknown	00-16-36-EB-E4-44	10.10.1.37	01:59:49
30	Unknown	00-16-36-C2-03-0F	10.10.1.38	01:59:50
31	Unknown	00-16-36-4A-2D-D9	10.10.1.39	01:59:51
32	Unknown	00-16-36-06-CF-94	10.10.1.40	01:59:52
33	Unknown	00-16-36-3D-26-05	10.10.1.41	01:59:53
34	Unknown	00-16-36-F4-92-62	10.10.1.42	01:59:54

Рисунок 48 – Заполнение всех доступных IPv4-адресов в DHCP-сервере

На Kali Linux разворачиваем DHCP-сервер. Для установки вводим команду apt-get install isc-dhcp-server.

После установки производим настройки DHCP-сервера. Перейдем по адресу: /etc/network/interfaces. Пропишем (рисунок 49):

auto eth0

iface eth0 inet dhcp

Рисунок 49 – Настройка DHCP-сервера

Перейдем по адресу: /etc/default/isc-dhcp-server. В строке «#INTERFACESv4=«"» уберем «#» и в скобках впишем eth0. Конечный результат будет выглядеть как на рисунке 50.

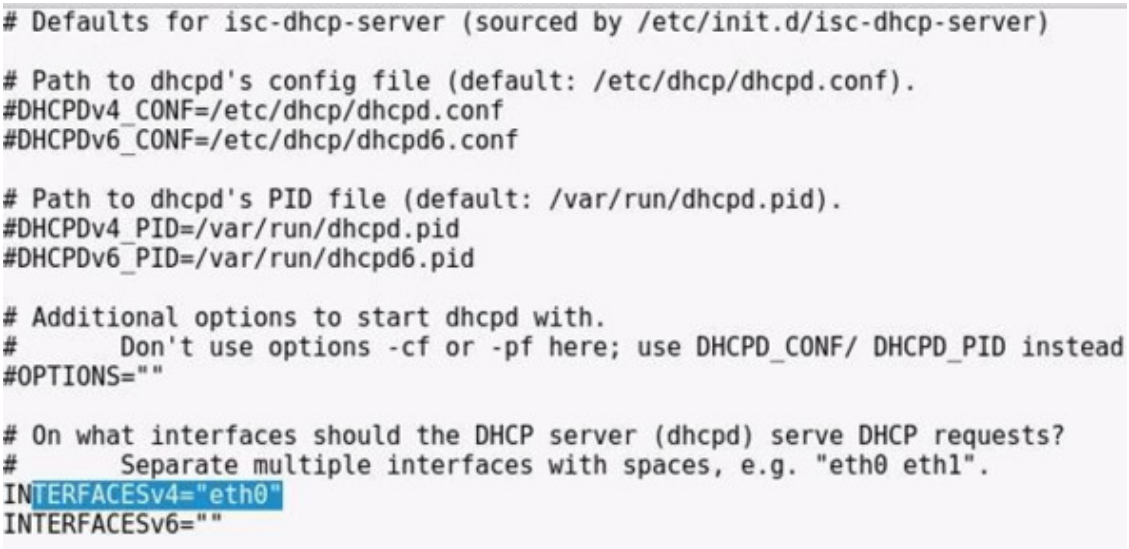


Рисунок 50 – Настройка DHCP-сервера

Перейдем по адресу: /etc/dhcp/dhcpd.conf. Ищем строку # This is a very basic subnet declaration. Настраиваем как на рисунке 51.

```
subnet 10.10.1.0 netmask 255.255.255.0 {
  range 10.10.1.100 10.10.1.200;
  option routers 10.10.1.10;
  option broadcast-address 10.10.1.255;
}
```

Рисунок 51 – Настройка DHCP-сервера

В нашем случае для правильной работы следует прописать следующие значения:

• subnet – IPv4-адрес сети;

• netmask – маска сети;

• range – пул адресов, которые будут выдаваться устройству при подключении к DHCP-серверу;

– option routers 10.10.1.10 – шлюз по умолчанию. В нашем случае необходимо указать IPv4-адрес устройства, в котором устанавливается DHCP-
сервер. Эту информацию можно посмотреть в ifconfig;

– option broadcast-address 10.10.1.255 – широковещательный адрес.

Для запуска DHCP-сервера вводим команду /etc/init. d/isc-dhcp-server start (рисунок 52).

```
root@kali:~# /etc/init.d/isc-dhcp-server start
[ ok ] Starting isc-dhcp-server (via systemctl): isc-dhcp-server.service.
```

Рисунок 52 – Ввод команды для запуска DHCP-сервера

После этого DHCP-сервер функционирует и может выдавать IPv4-адреса узлам, которые пытаются подключится к роутеру.

Подключаем другое устройство к роутеру. В нашем случае – это смартфон. После подключения он получает IPv4-адрес из пула адресов, назначенных на DHCP-сервере атакующего (рисунок 53).

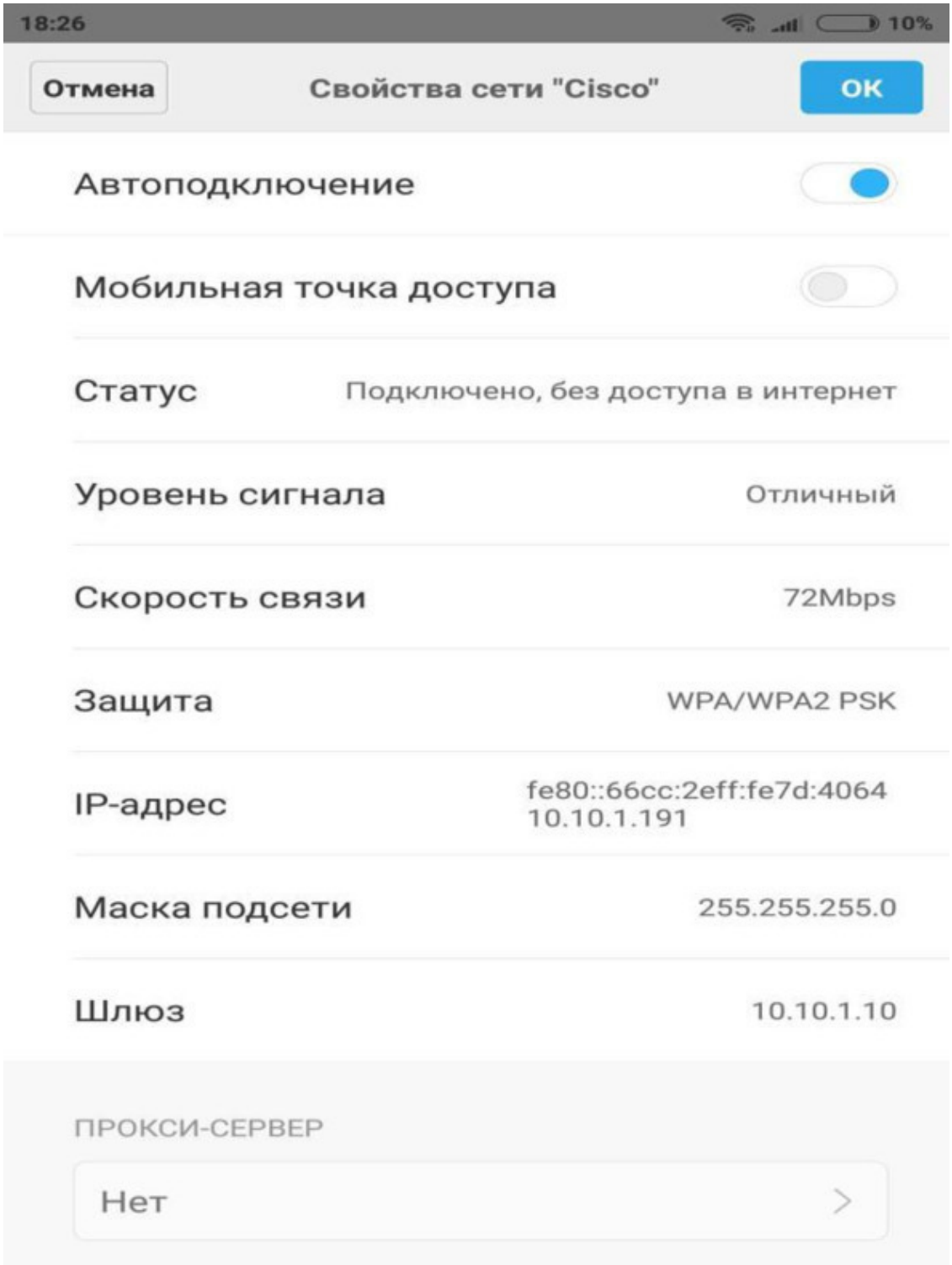


Рисунок 53 – Получение IPv4-адреса из пула адресов

IPv4-адрес смартфона в нашем случае: 10.10.1.191 (адрес получен от DHCP-сервера атакующего). IPv4-адрес компьютера, к которому отправляются Echo-запросы для проверки соединения имеет адрес 10.10.1.70, как на рисунке (IPv4-адрес получен от настоящего DHCP-сервера, который был на роутере). На рисунках 54—55 показаны Echo-запросы от одного устройства к другому.

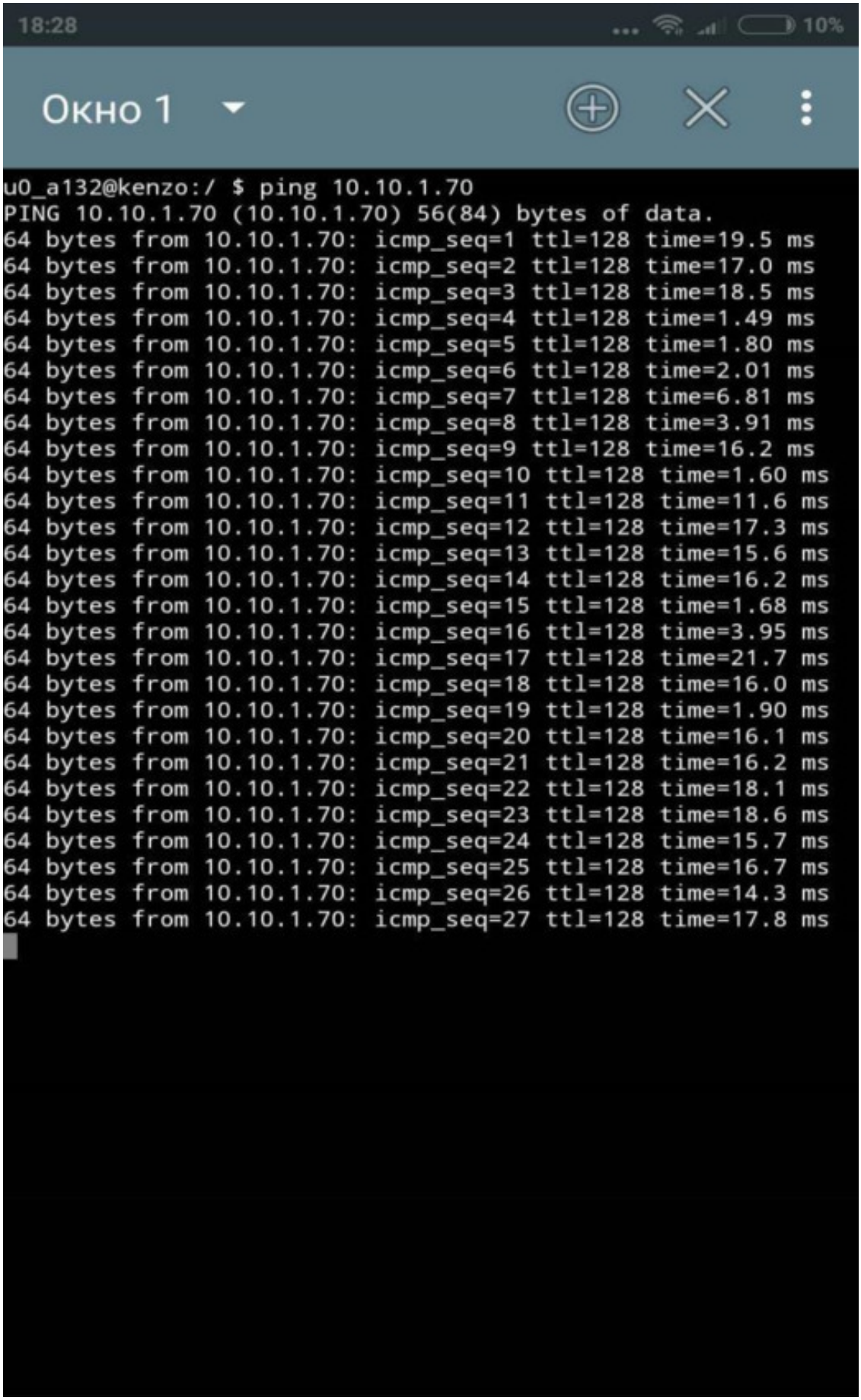


Рисунок 54 – Echo-запросы

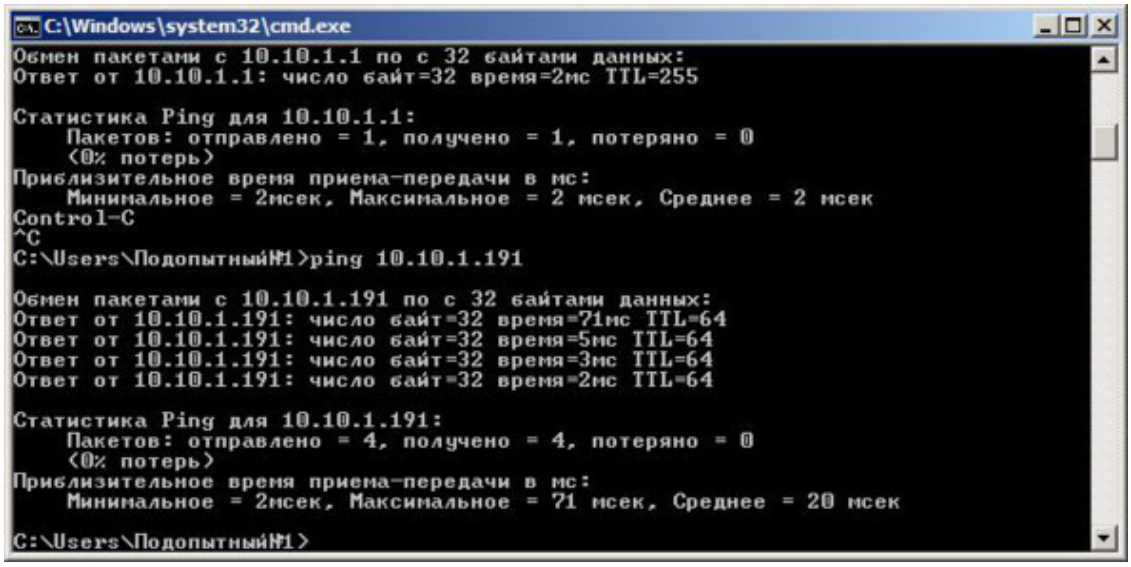


Рисунок 55 – Echo-запросы

Во время Echo-запросов Wireshark, запущенный под управлением Kali Linux, получает пакеты, которые передавались от одного устройства к другому. Следовательно, правильно произвести атаку нам удалось.

3. DoS

Основная идея, что большой наплыв пользователей приводит к отказу в обслуживании части из них. Расширение данной атаки – DDOS.

Для реализации нескольких типов DDoS-атак соберем лабораторный стенд по рисунку 56. Атакующих компьютеров необязательно должно быть 10 – можно ограничиться 2—3 компьютерами, которые будут атаковать сервер.

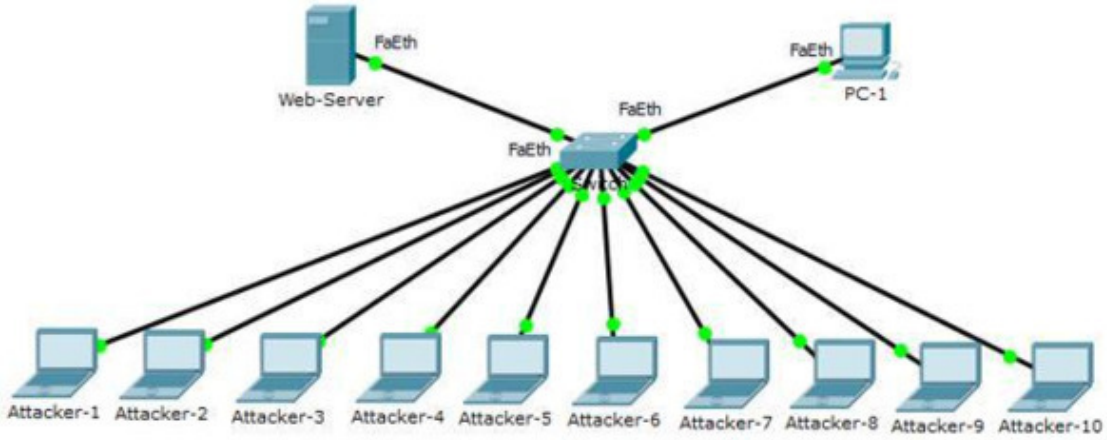


Рисунок 56 – Схема лабораторного стенда

3.1 HTTP-флуд

HTTP-флуд – это наиболее распространенная flood-атака. В ее основе – отсылка HTTP-запросов GET на 80-й порт и, как следствие, переполнение и невозможность обрабатывать новые запросы.

Для реализации этой и последующих типов атак мы воспользуемся программой Low Orbit Ion Cannon. LOIC – программа с открытым исходным кодом, предназначенная для осуществления DDoS-атак, написанная на языке программирования C#.

Запускаем программу на компьютерах атакующих (рисунок 57).

Рисунок 57 – Интерфейс программы Low Orbit Ion Cannon

Настраиваем программу следующим образом:

В «1. Select your target» прописываем в нужную строку либо известный адрес

Нажимаем кнопку «Lock on»; В «3. Attack options» выставляем метод HTTP, количество потоков для атаки, убираем галочку «Wait for reply»; в «2. Ready?» нажимаем кнопку «IMMA CHARGIN MAH LAZER».

Во время атаки сервер жертвы получает огромную нагрузку на процессор. Через некоторое время сервер становится недоступным – появляется 503 ошибка (рисунок 58).

Рисунок 58 – ошибка 503

Реализация в LOIC TCP и UDP flood атак выполняется аналогичным образом: в качестве метода в программе выбирается либо TCP-, либо UDP-атака. Конечно, если злоумышленник получит шелл, то он может реализовать атаку типа недостатка ресурсов переполнив процессор ненужными инструкциями или память ненужными вычислениями.

На рисунке 59 показан скриншот из Диспетчера задач атакованного сервера. Видно, что сервер испытал большую нагрузку во время расчетов.

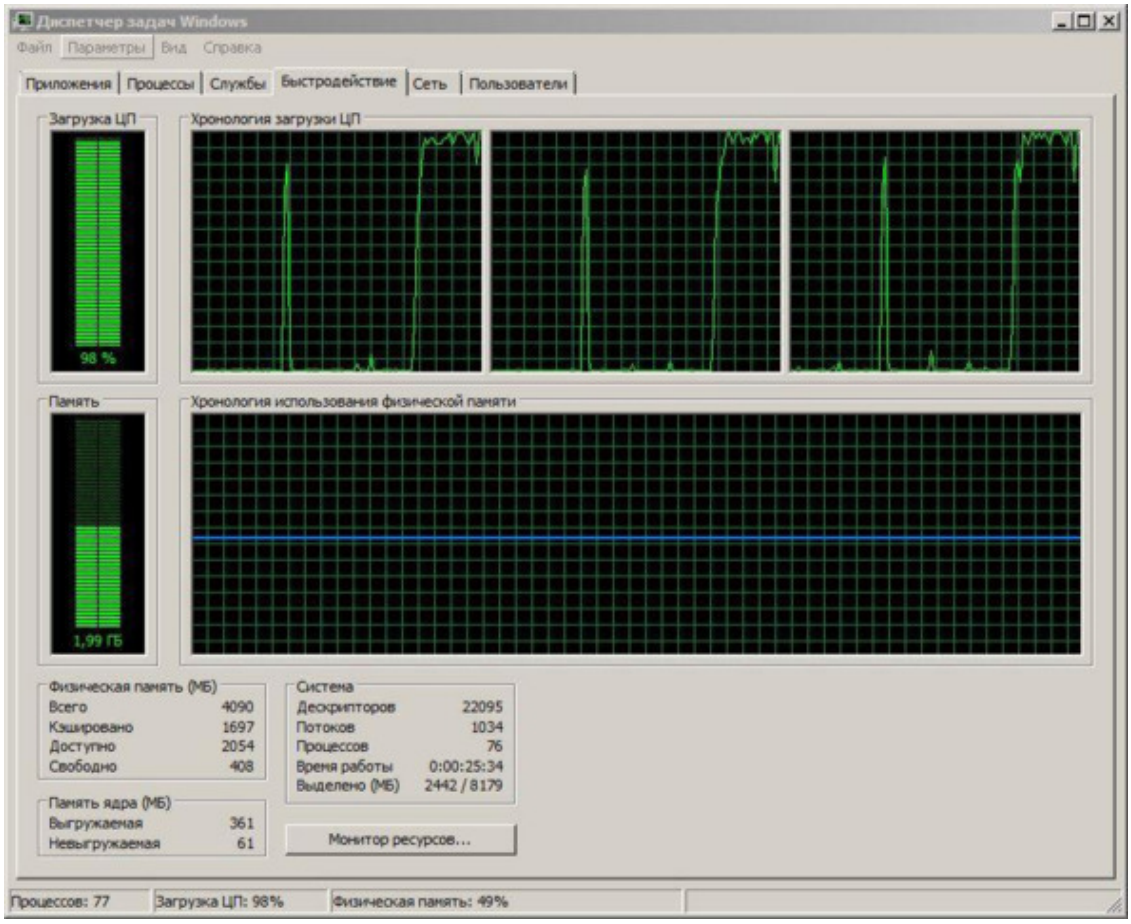


Рисунок 59 – Диспетчер задач атакованного сервера

Атаки на программное обеспечение

Использование IDA Pro в зада

IDA Pro Disassembler (Interactive DisAssembler) – наиболее популярное средство на рынке сегодня. Это интерактивный дизассемблер, широко использующийся для обратной разработки программ позволяющий итеративно исследовать исходный код, пока не станет ясно, что именно и как делает исследуемая программа.

Существует несколько версий IDA Pro – бесплатная (freeware), стандартная (standard) и расширенная (advanced). Бесплатная версия обладает ограниченными возможностями по сравнению со стандартной и расширенной версиями – поддерживается только архитектура x86 и отсутствует поддержка подключаемых модулей.

1 Использование IDA Pro
1.1 Автоматический анализ

После запуска IDA предлагает 3 варианта продолжения: дизассемблировать новый файл (new), продолжить без загрузки файла (go), открыть ранее дизассемблированный файл (previous). Скриншот окна представлен на рисунке 60.

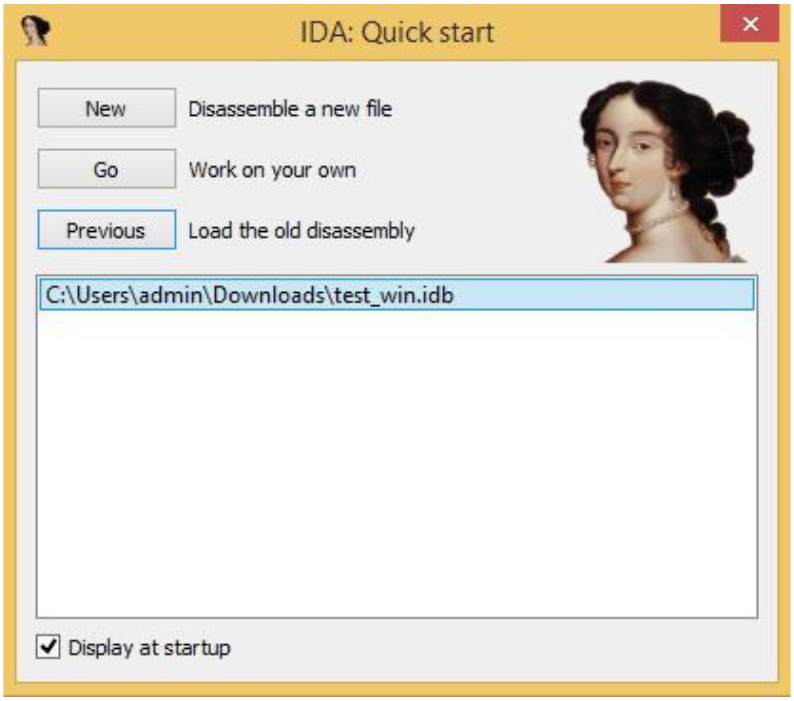


Рисунок 60 – Окно быстрого старта.

Выберем дизассемблирование нового файла. Загрузим на анализ любой exe. Далее появится окно, изображённое на рисунке 61.

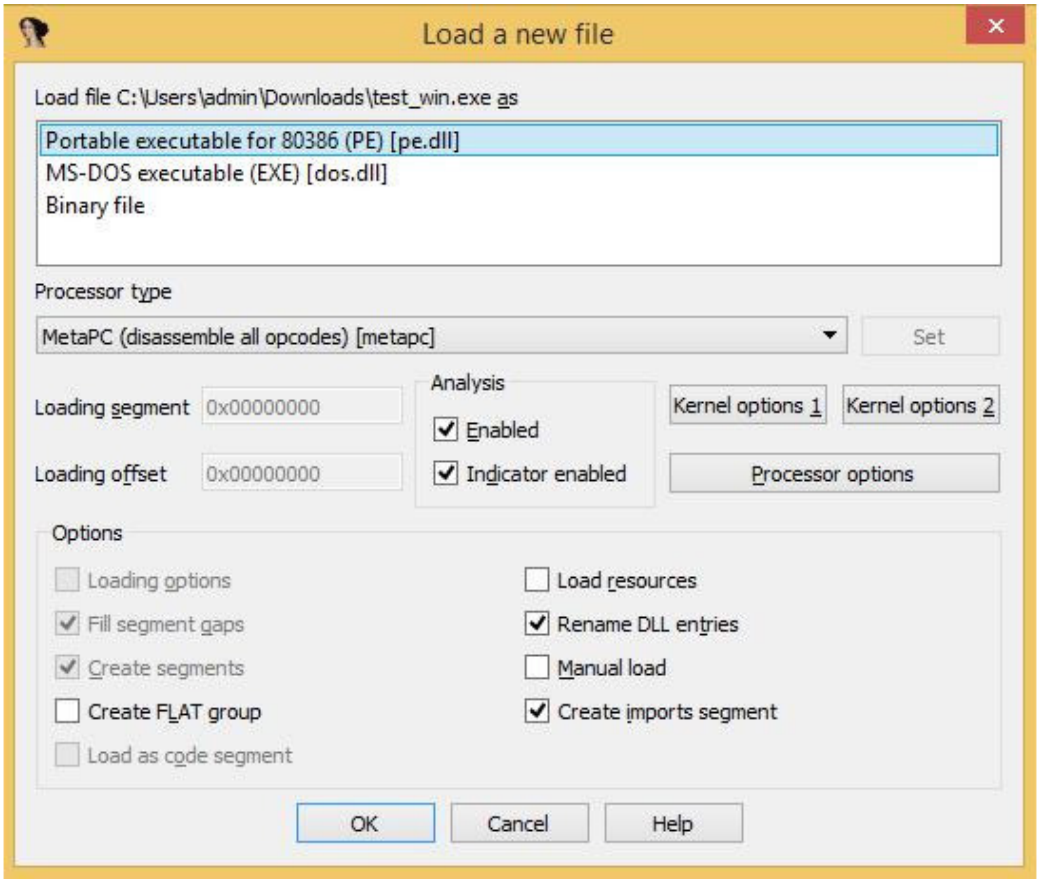


Рисунок 61 – Загрузка файла на анализ.

Иногда после компиляции в файле остаётся отладочная информация. Тогда IDA покажет окно, изображённое на рисунке 62 с предложением загрузить отладочную информацию.

Рисунок 62 – Загрузка отладочной информации.

После окончания автоматического анализа IDA покажет графовое представление функции, где находится точка входа (если она найдена), либо первой функции в файле.

Кроме графового представления существует множество других важных вкладок, доступных в меню View-> subviews: шестнадцатеричное представление, список строк в файле, список имён из библиотек или отладочной информации, список импортированных функций и значений с указанием библиотеки.

Кроме того, в IDA существует возможность представить функцию в виде псевдокода, синтаксис которого копирует синтаксис языка программирования Си. Для просмотра функции в виде псевдокода нужно нажать клавишу F5.

1.2 Ручной анализ

Качественное отличие IDA Pro от других дизассемблеров – интерактивность. Пользователь может сам сообщать дизассемблеру дополнительную информацию.

Рассмотрим метод ручного анализа на практике. Часто бывает так, что IDA не может в автоматическом режиме найти функцию main, которая чаще всего является точкой входа. Эта функция принимает два обязательных аргумента: argc (количество аргументов) и argv (список аргументов). То есть можно косвенно предположить что если функция в программе работает с этими аргументами то она и есть main.

Откроем вкладку списка имён. Нажатием Ctrl+F включаем поиск по именам.

С помощью поиска находим имена _argv и _argc. В IDA Pro есть функция просмотра ссылок на объект. Выбираем _argc (или _argv), нажимаем клавишу X. Появляется окно ссылок.

1.3 Отладка

В составе IDA Pro дополнительно есть отладчик. Он позволяет пошагово выполнять программу, исследовать и модифицировать память во время выполнения программы.

Панель запуска отладки находится в верхней части окна, она изображена на рисунке 63. С её помощью можно запустить отладку, приостановить отладку, остановить отладку. Также можно выбрать отладчик (локальная машина, виртуальная машина, удалённая машина).

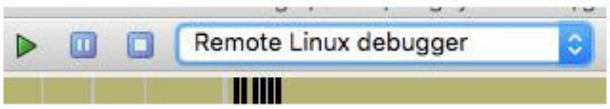


Рисунок 63 – Панель отладки.

Для исследования программы в нужном месте следует использовать точки остановы (breakpoints). Они устанавливаются с помощью панели, которая находится справа от панели отладки. Панель содержит стандартные функции по работе с точками останова.

При запуске программы она выполнится до точки остановы и будет ожидать дальнейших действий пользователя. Затем программу можно выполнять в таком же режиме (до следующей точки остановы), для этого нужно нажать кнопку запуска отладки. Либо можно исследовать программу, выполняя её пошагово. Для этого существуют команды step into (шаг со входом в функцию, F7) и step over (шаг без входа, F8).

Исследуя код можно заметить, что при некотором условии на экран будет выводиться строка та или иная строка. Также мы знаем, что за сравнения в языке ассемблера отвечает инструкция cmp. IDA позволяет редактировать программу в процессе выполнения. Для этого

выбираем нужную часть кода, выбираем Edit -> Patch Program -> Assembly. И пишем нужную часть кода.

Конец ознакомительного фрагмента.