

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Лабораторная работа №2

Авторизация сетевых соединений

Выполнили студенты группы ИКТЗ-83:

Громов А.А., Миколаени М.С., Мазеин Д.С.

(Ф.И.О., № группы)

(подпись)

Проверил:

Казанцев А.А.

(уч. степень, уч. звание, Ф.И.О.)

(подпись)

Санкт-Петербург

2021

Пункт 2

В данном пункте мы убедились, что передается открытый трафик с помощью программы Wireshark.

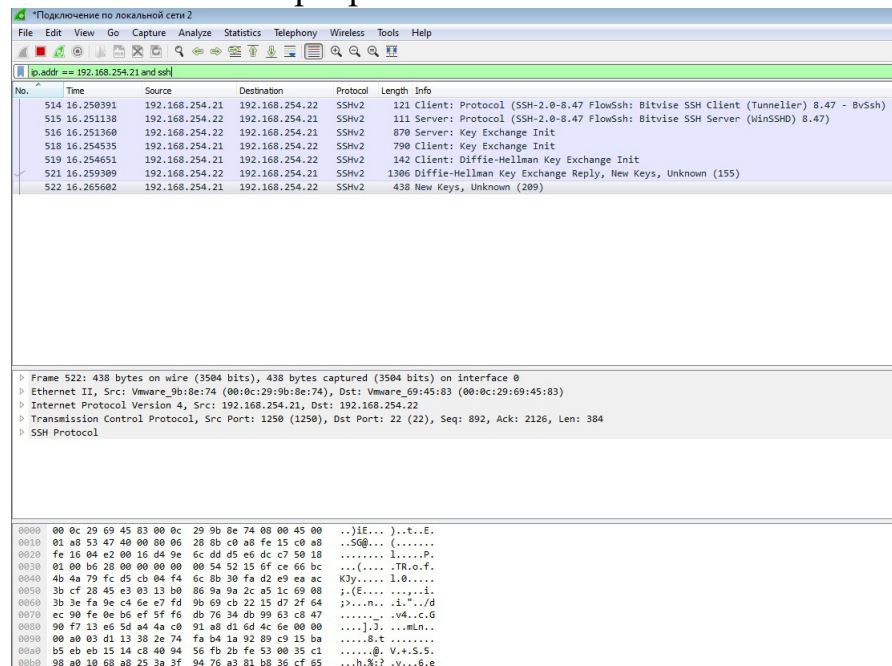


Рис. 1 Открытый трафик.

Пункт 3

В данном пункте мы настроили правила доступа, разрешающее всем сетевым сервисам входящее подключение.

| Правила доступа | | | | | | |
|---|----------|-------------------|-------------------------|-------------|-----------------|------------|
| Правила, регламентирующие доступ к сетевым сервисам (TCP/IP v4) данного компьютера. | | | | | | |
| Вкл | Субъект | Сетевой сервис | Тип доступа | Направление | Удаленный адрес | Приложение |
| <input checked="" type="checkbox"/> | everyone | Secret Net Studio | Все входящие (UDP, TCP) | Разрешен | Входящее | * |

Рис. 2 Парвило доступа.

Пункт 4

В данном пункте мы настроили режим защиты сетевых соединений.

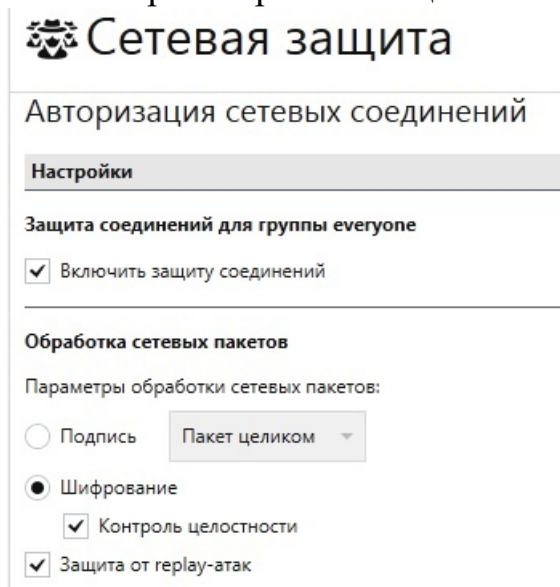


Рис. 3 Экран настроек.

Пункт 5

В данном пункте мы убедились, что передается зашифрованный трафик

File Edit View Go Capture Analyze Statistics Help

ip.addr == 192.168.254.21 and ssh

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|----------------|----------------|----------|--------|--|
| 514 | 16.250391 | 192.168.254.21 | 192.168.254.22 | SSHv2 | 121 | Client: Protocol (SSH-2.0-8.4.7 FlowSsh; Bitwise SSH Client (Tunneller) 8.4.7 - BvSSH) |
| 516 | 16.251138 | 192.168.254.22 | 192.168.254.21 | SSHv2 | 111 | Server: Protocol (SSH-2.0-8.4.7 FlowSsh; Bitwise SSH Server (WinSSHD) 8.4.7) |
| 518 | 16.251368 | 192.168.254.21 | 192.168.254.21 | SSHv2 | 870 | Server: Key Exchange Init |
| 519 | 16.254535 | 192.168.254.21 | 192.168.254.22 | SSHv2 | 790 | Client: Key Exchange Init |
| 519 | 16.254651 | 192.168.254.21 | 192.168.254.22 | SSHv2 | 142 | Client: Diffie-Hellman Key Exchange Init |
| 521 | 16.259309 | 192.168.254.22 | 192.168.254.21 | SSHv2 | 1306 | Diffie-Hellman Key Exchange Reply, New Keys, Unknown (155) |
| 522 | 16.265602 | 192.168.254.21 | 192.168.254.22 | SSHv2 | 438 | New Keys, Unknown (209) |
| 2211 | 445.316954 | 192.168.254.21 | 192.168.254.22 | SSHv2 | 121 | Client: Protocol (SSH-2.0-8.4.7 FlowSsh; Bitwise SSH Client (Tunneller) 8.4.7 - BvSSH) |
| 2212 | 445.317069 | 192.168.254.22 | 192.168.254.21 | SSHv2 | 111 | Server: Protocol (SSH-2.0-8.4.7 FlowSsh; Bitwise SSH Server (WinSSHD) 8.4.7) |
| 2213 | 445.318115 | 192.168.254.21 | 192.168.254.21 | SSHv2 | 870 | Server: Key Exchange Init |
| 2215 | 445.321405 | 192.168.254.21 | 192.168.254.22 | SSHv2 | 790 | Client: Key Exchange Init |
| 2216 | 445.321406 | 192.168.254.21 | 192.168.254.22 | SSHv2 | 142 | Client: Diffie-Hellman Key Exchange Init |
| 2218 | 445.327230 | 192.168.254.22 | 192.168.254.21 | SSHv2 | 1306 | Diffie-Hellman Key Exchange Reply, New Keys, Unknown (104) |
| 2219 | 445.331289 | 192.168.254.21 | 192.168.254.22 | SSHv2 | 438 | New Keys, Unknown (13) |

```

Frame 2219: 438 bytes on wire (3504 bits), 438 bytes captured (3504 bits) on interface 0
Ethernet II, Src: VMware_08:0e:74:00:c8:29:90:0e:74), Dst: VMware_69:45:a8:00:8c:29:69:45:b3)
Internet Protocol Version 4, Src: 192.168.254.21, Dst: 192.168.254.22
Transmission Control Protocol, Src Port: 1265 (1265), Dst Port: 22 (22), Seq: 892, Ack: 2126, Len: 384
SSH Protocol
    
```

```

0000 00 8c 29 69 45 b3 00 0c      29 9b fe 74 08 00 45 00   ..)IE...).t..E.
0010 01 8d 54 91 40 00 80 06     27 41 c0 a8 fe 15 c0 a8   .T.B@....fe l5 c0 a8
0020 fe 16 04 f1 00 16 33 3d     98 1e 25 d3 ca 14 50 18   ....3=..X.P.F.
0030 01 00 e7 50 00 00 00 00     00 54 15 b9 ad 27 bf     .....TR.....
0040 71 9e 1a f1 c3 0e 8d 51     5d 2e 3b 92 46 cd 37     q.....Q|.Z.F.T.
0050 3b d6 c4 e4 57 01 3f 05     c6 91 be df 82 b9 aa 09   j.WN?P.....
0060 1b ec 25 19 f1 75 2e 61     04 87 64 b4 21 9c 81 81   .X.u.a..d.l..
0070 1e 5d 5e b2 18 f2 5f 41     c3 0a 08 00 ee 41 6e     |.....A.....
0080 fc 58 b9 dc ee 67 98 e1     59 07 d7 b8 ce e1 00 00   X..g..Y.....
0090 00 a0 61 dd 08 bc 9a 36     a9 0a 03 1b 30 2d fb ff   ..a...6...0...
00a0 20 e1 4e bb b2 7c 06 70     6c df 69 2b ba 4e 00 05   .W|..p.l.t.M..
00b0 73 53 ed 2a 02 07 fd 9d     0b eb 09 e5 94 04 54     s.....T.....
    
```

wreshark packet F6066464-527B-46BC-9FCE-AB49313BF614 2024.10.19.16.1907.400034

Рис. 4 Не удалось зашифровать трафик.

Пункт 7

В данном пункте мы настроили блокировку соединений для неавторизованных на СБ пользователей

Сетевая защита

Персональный межсетевой экран

Правила доступа

Правила, регламентирующие доступ к [сетевым сервисам](#) (TCP/IP v4) данного компьютера.

| Вкл | Субъект | Сетевой сервис | Тип доступа | Направление | Удаленный адрес | Приложение |
|-------------------------------------|----------------------------|-------------------------|-------------|-------------|-----------------|------------|
| <input checked="" type="checkbox"/> | anonymous Secret Net Studi | Все входящие (UDP, TCP) | Запрещен | Входящее | * | * |

Рис. 5 Парвило доступа.

Вывод

Выполнив данную лабораторную работу, мы протестировали компонент "Авторизация сетевых соединений" в Secret Net Studio. Нами была реализована защита протокола SSH от перехвата передаваемых по нему данных.

Ответы на контрольные вопросы.

- 1. В чем заключается особенность функционирования ПМЭ в Secret Net Studio, отличающая его от традиционных, "периметровых" МЭ?**

В отличие от традиционных, "периметровых" МЭ, реализованный в SNS распределенный межсетевой экран предназначен именно для защиты информации внутри сети организации, функционирует непосредственно на ее защищаемых объектах (сервер БД, рабочие места руководителей или сотрудников и т.д.) и обеспечивает их защиту от сетевых угроз со стороны внешнего и внутреннего нарушителей.

- 2. Какие группы правил проверки сетевого трафика реализованы в ПМЭ Secret Net Studio?**

Правила доступа, прикладные правила, системные правила, сетевые протоколы.

- 3. Какая из групп правил проверки сетевого трафика в ПМЭ Secret Net Studio имеет наивысший приоритет? Что регламентируется правилами этой группы?**

Системные правила

- 4. По каким протоколам может ограничиваться доступ к защищаемым ресурсам с помощью системных правил?**

Все IP-based протоколы (RDP)

- 5. Какая из групп правил проверки сетевого трафика в ПМЭ Secret Net Studio имеет минимальный приоритет? Что регламентируется правилами этой группы?**

Прикладные правила. Регламентируют доступ пользователей к сетевым сервисам защищаемого компьютера (например, общие папки).

- 6. Каков порядок обработки заданных в параметрах ПМЭ Secret Net Studio правил доступа?**

Чем выше правило в таблице, тем больше его приоритет

- 7. Через какой промежуток времени после сохранения изменений вступают в силу новые настройки правил доступа ПМЭ Secret Net Studio?**

4 - 6 минут

- 8. Какой режим работы ПМЭ в Secret Net Studio позволяет составить на основе информации о сетевой активности приложений базовый набор правил доступа, необходимый для функционирования защищаемого компьютера?**

Сетевой режим

9. В чем заключается особенность аутентификации пользователей механизмом авторизации сетевых соединений Secret Net Studio?

Механизм авторизации сетевых соединений обеспечивает защиту взаимодействия только между авторизованными на СБ клиентами Secret Net Studio. Если на компьютере пользователя не установлен Secret Net Studio или пользователь по каким-либо причинам не прошел аутентификацию на СБ SNS (anonymous), то трафик между ним и авторизованным клиентом SNS не будет защищаться.

10. Какими средствами обеспечивается защита и целостность передаваемых данных в механизме авторизации сетевых соединений?

Средствами протоколов семейства IPsec, а именно АН (Authentication Header) - гарантирует аутентичность и целостность и ESP (Encapsulation Security Payload) - шифрование и контроль целостности.

11. Что необходимо для возможности выбора пользователя или группы пользователей, доступ к которой будет контролироваться при создании нового правила доступа в параметрах настроек политик ПМЭ?

Необходима лицензия на использование механизма авторизации сетевых соединений.

12. Наличие каких правил необходимо для работы прикладных правил доступа к общим папкам на защищаемом компьютере?

Если прохождение пакетов по протоколу SMB запрещается системными правилами или правилами доступа, то прикладные правила не работают, так как на транспортном уровне IP-пакеты блокируются.