Липецкий государственный технический университет

Факультет автоматизации и информатики

Кафедра Автоматизированных систем управления

Отчет по лабораторной работе № 7

«Работа с SSH»

по курсу «ОС Linux»

Студент Грунау Г. Ю.

Группа АИ-18

Руководитель Кургасов В. В.

Липецк 2021 г.

Цель работы

Лабораторная работа предназначена для целей практического ознакомления с программным обеспечением удаленного доступа к распределённым системам обработки данных.

Выполнение работы

Запустим терминальный мультиплексор tmux и создадим новое окно, в котором запустим анализатор трафика tcpdump с фильтром пакетов получаемых и передаваемых от узла domen.name с TCP-портом источника и назначения 23. С помощью команды tee, вывести отфильтрованные IP-пакеты на терминал и сохранить данные в файл telnet.log, в домашнем каталоге пользователя. Для этого следует воспользоваться командой

sudo tcpdump -l -v -nn tcp and src port 23 or dst port 23 | tee telnet.log

```
lovediehate@ubser:~$ sudo tcpdump -l -v -nn tcp and src port 22 or dst port 22
| tee telnet.log;
[sudo] password for lovediehate:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144
bytes
```

Рисунок 1 – Анализатор трафика telnet

Установим соединение с удаленным сервером по протоколу TELNET.

```
lovediehate@ubser:~$ telnet 178.234.29.197 22
Trying 178.234.29.197...
Connected to 178.234.29.197.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.10
Connection closed by foreign host.
```

Рисунок 2 – Попытка соединения

```
10:11:57.743206 IP (tos 0x10, ttl 64, id 29692, offset 0, flags [DF], proto TCP
 (6), length 60)
    10.0.2.15.44374 > 178.234.29.197.22: Flags [S], cksum 0xdcec (incorrect ->
0xd44a), seq 3533098519, win 64240, options [mss 1460,sackOK,TS val 4173616422
ecr 0,nop,wscale 7], length 0
10:11:57.780814 IP (tos 0x0, ttl 64, id 746, offset 0, flags [none], proto TCP
(6), length 44)
    178.234.29.197.22 > 10.0.2.15.44374: Flags [S.], cksum 0x37a3 (correct), se
q 26752001, ack 3533098520, win 65535, options [mss 1460], length 0
10:11:57.780848 IP (tos 0x10, ttl 64, id 29693, offset 0, flags [DF], proto TCP
 (6), length 40)
    10.0.2.15.44374 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect ->
0x546f), ack 1, win 64240, length 0
10:11:57.825070 IP (tos 0x0, ttl 64, id 747, offset 0, flags [none], proto TCP
(6), length 82)
    178.234.29.197.22 > 10.0.2.15.44374: Flags [P.], cksum 0x28d9 (correct), se
q 1:43, ack 1, win 65535, length 42
10:11:57.825092 IP (tos 0x10, ttl 64, id 29694, offset 0, flags [DF], proto TCP
 (6), length 40)
    10.0.2.15.44374 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect ->
0x546f), ack 43, win 64198, length 0
```

Рисунок 3 – Логи подключения

Как мы видим на рисунке 2 соединение было установлено, однако сервер не предлагает нам пройти авторизацию. А также на рисунке 3 в окне с анализатором трафика можно понять по отфильтрованным ip-пакетам, что подключение было успешным.

Теперь запустим анализатор трафика по порту 22, но с файлом ssh.log

```
lovediehate@ubser:~$ sudo tcpdump -l -v -nn tcp and src port 22 or dst port 22
| tee ssh.log;
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144
bytes
```

Рисунок 4 – Анализатор трафика ssh

```
lovediehate@ubser:~$ ssh -l stud2 178.234.29.197
stud2@178.234.29.197's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-193-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

     https://microk8s.io/high-availability

12 packages can be updated.
0 updates are security updates.


*** Требуется перезагрузка системы ***
Last login: Tue Feb  2 00:37:40 2021 from 176.212.145.54
```

Рисунок 5 – Подключение к удалённому узлу по SSH

В окне с анализатором трафика можно увидеть логи успешного подключения с отфильтрованными по 22 порту ip-пакетами.

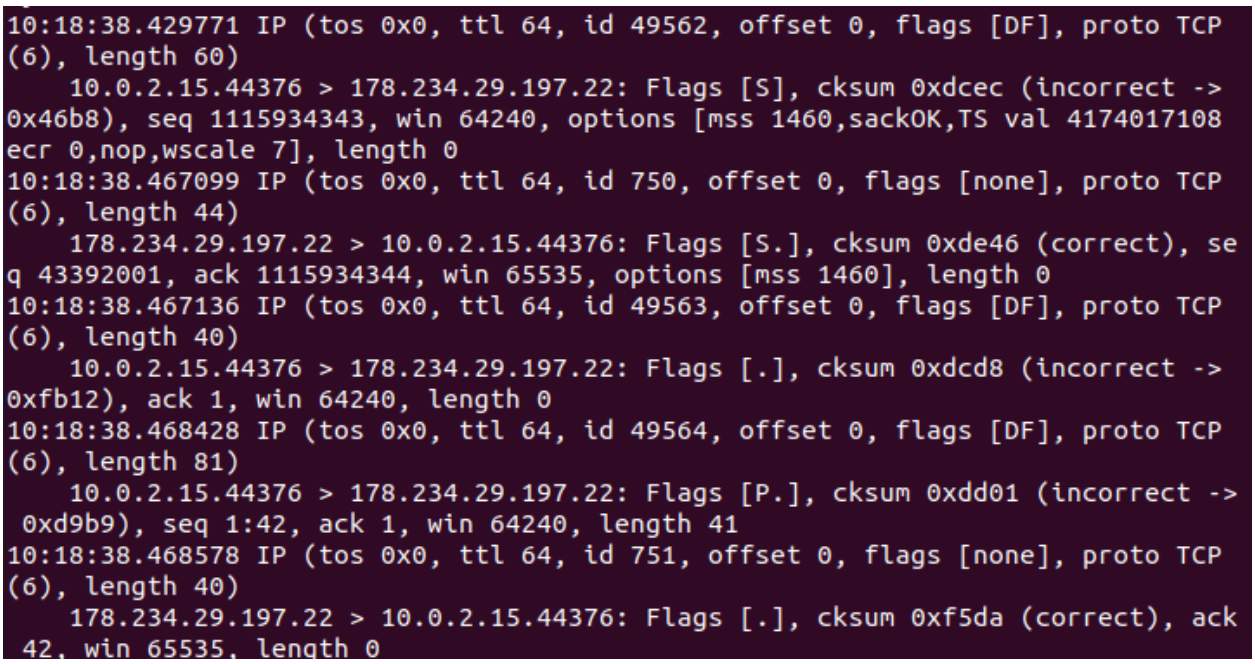

Рисунок 6 – Логи из ssh.log

Выполнив команду uname –a в удаленном узле, можно получить информацию о нём:

Рисунок 7 – Информация об удалённой системе

Теперь откроем новое окно для того, чтобы создать файл с содержанием требуемой информации в нашей локальной системе.

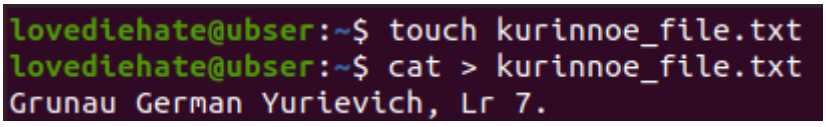

Рисунок 8 – Текстовый файл

С помощью команды scp filename login@domenname:/home/stud2 передадим наш файл по шифрованному каналу.

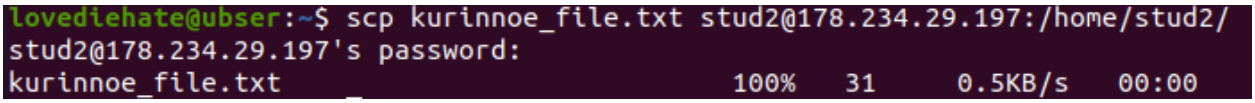

Рисунок 9 – Передача файла

С помощью команды mc на удаленном узле можно проверить файл.

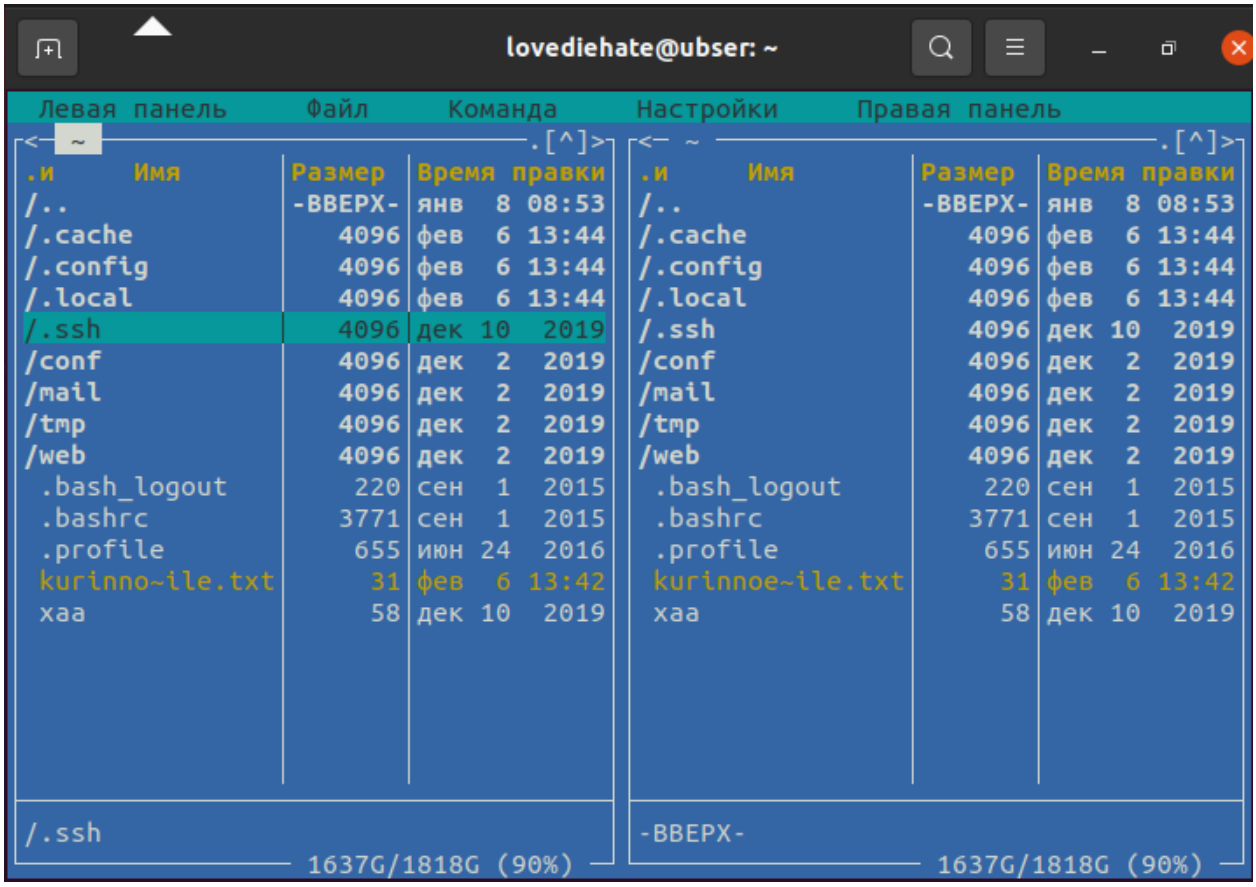

Рисунок 10 – Переданный файл на удаленном узле

```
$ exit
Connection to 178.234.29.197 closed.
lovediehate@ubser:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/lovediehate/.ssh/id_rsa):
/home/lovediehate/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/lovediehate/.ssh/id_rsa
Your public key has been saved in /home/lovediehate/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:5g/drk61I6tBOchYWHOtTUaykMwI+n50GGtzG4b7VbI lovediehate@ubser
The key's randomart image is:
+---[RSA 3072]----+
|  .. ++.oo.      |
| .  .o++ o+      |
|.   o . .=       |
| .   O ....      |
|  . O B S . .    |
| . o * * * o .   |
|  . o . E + +    |
|   . . . = + .   |
|      . .o=..    |
+----[SHA256]-----+
```

Рисунок 11 – Генерация ключа

На рисунке 11 изображена генерация публичного и приватного ключей SSH.

С помощью команды scp передадим сгенерированный публичный ключ на локальный узел, предварительно переименовав его в authorized_keys

```
lovediehate@ubser:~/.ssh$ scp autorized_keys stud2@178.234.29.197:/home/stud2/.
ssh/
Enter passphrase for key '/home/lovediehate/.ssh/id_rsa':
stud2@178.234.29.197's password:
autorized_keys                                100%  571    10.3KB/s   00:00
```

Рисунок 12 – Передача ключей

Снова сделаем попытку подключения к удаленному узлу:

```
Enter passphrase for key '/home/lovediehate/.ssh/id_rsa':
stud2@178.234.29.197's password:
autorized_keys                                100%  571    10.3KB/s   00:00
lovediehate@ubser:~/.ssh$ ssh -l stud2 178.234.29.197
Enter passphrase for key '/home/lovediehate/.ssh/id_rsa':
stud2@178.234.29.197's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-193-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

     https://microk8s.io/high-availability

12 packages can be updated.
0 updates are security updates.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** Требуется перезагрузка системы ***
Last login: Sat Feb  6 13:18:59 2021 from 176.212.145.54
```

Рисунок 13 – Подключение к удаленной системе

Теперь система помимо пароля запросила у меня кодовое слово для приватного ключа, которое я вводил при генерации шифров.

Попробуем ещё раз передать файл с локальной системы, переименовав его:

```
lovediehate@ubser:~/.ssh$ mv autorized_keys die
lovediehate@ubser:~/.ssh$ scp die stud2@178.234.29.197:/home/stud2/
Enter passphrase for key '/home/lovediehate/.ssh/id_rsa':
stud2@178.234.29.197's password:
die                                           100%  571    10.1KB/s   00:00
```

Рисунок 14 – Передача файла

Система запросила у меня кодовое слово, которое я указал при генерации.

Проверим наличие файла, авторизовавшись в системе и выполнив команду **mc**.

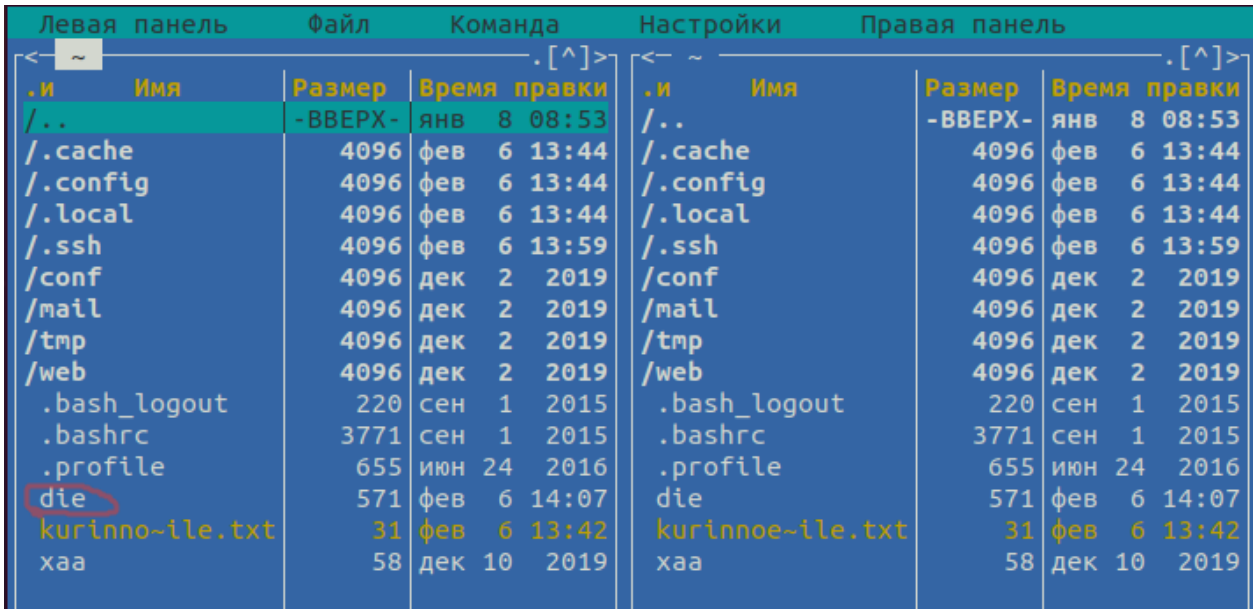

Рисунок 15 – Наличие файла в удаленной системе

Теперь приостановим работу анализатора трафика с помощью комбинации ctrl+c:

```
^C1430 packets captured
1430 packets received by filter
0 packets dropped by kernel
```

Рисунок 16 – Завершение процесса