

Липецкий государственный технический университет

Кафедра прикладной математики

Отчет по лабораторной работе № 7
«Авторизация по ключу SSH»
по курсу «Операционная система Linux»

Студент

подпись, дата

Сергеев Е.С.
фамилия, инициалы

Группа ПМ-19-2

Руководитель

Доцент, к. пед. наук
ученая степень, ученое звание

подпись, дата

Кургасов В.В.
фамилия, инициалы

Липецк 2021 г.

Содержание

Цель работы	3
1. Ход работы	4
1.1. Запуск анализатора трафика tcpdump (порт 23)	4
1.2. Попытка установки соединения (порт 23)	5
1.3. Запуск анализатора трафика tcpdump (порт 22)	6
1.4. Попытка установки соединения (порт 22)	7
1.5. Запуск анализатора трафика tcpdump (порт 22)	8
1.6. Установление шифрованного соединения с удаленным сервером	9
1.7. Вывод информации об удаленной системе	10
1.8. Передача файла по шифрованному каналу	11
1.9. Формирование зашифрованных ключей	12
1.10. Передача публичного ключа	13
1.11. Подключение к удаленной системе	14
1.12. Передача файла по шифрованному каналу	15
1.13. Содержимое файла telnet.log	16
Вывод	17

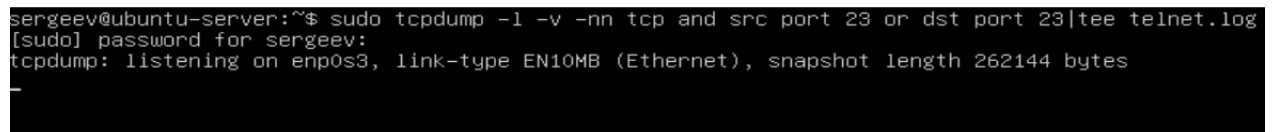
Цель работы

Организовать доступ к удаленному серверу по ssh (без ввода пароля (по ключу)) имея следующие исходные данные:

- IP: 178.234.29.197
- Порт: 22
- Логин: stud9
- Пароль: rV6MBb6zgC

1. Ход работы

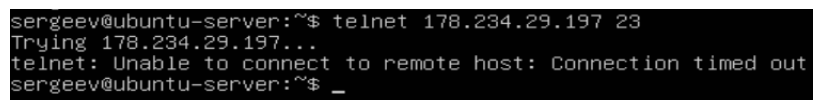
1.1. Запуск анализатора трафика tcpdump (порт 23)



```
sergeev@ubuntu-server:~$ sudo tcpdump -i -v -nn tcp and src port 23 or dst port 23|tee telnet.log
[sudo] password for sergeev:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
-
```

Рисунок 1 – Запуск анализатора трафика tcpdump.

1.2. Попытка установки соединения (порт 23)

A terminal window with a black background and white text. The text shows a user named 'sergeev' on an 'ubuntu-server' machine attempting to connect to the IP address '178.234.29.197' on port '23' using the 'telnet' command. The output shows the connection attempt, the IP being tried, and a timeout error message: 'telnet: Unable to connect to remote host: Connection timed out'. The prompt returns to the shell.

```
sergeev@ubuntu-server:~$ telnet 178.234.29.197 23
Trying 178.234.29.197...
telnet: Unable to connect to remote host: Connection timed out
sergeev@ubuntu-server:~$ _
```

Рисунок 2 – Попытка установки соединения.

23 порт недоступен.

1.3. Запуск анализатора трафика tcpdump (порт 22)

```
sergeev@ubuntu-server:~$ sudo tcpdump -i -v -nn tcp and src port 22 or dst port 22 | tee telnet.log
[sudo] password for sergeev:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
-
```

Рисунок 3 – Запуск анализатора трафика tcpdump.

1.4. Попытка установки соединения (порт 22)

```
sergeev@ubuntu-server:~$ 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 4 – Попытка установки соединения.

22 порт недоступен.

1.5. Запуск анализатора трафика tcpdump (порт 22)

```
sergeev@ubuntu-server:~$ sudo tcpdump -i -v -nn tcp and src port 22 or dst port 22|tee ssh.log  
[sudo] password for sergeev:  
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Рисунок 5 – Запуск анализатора трафика tcpdump.

1.6. Установление шифрованного соединения с удаленным сервером

```
sergeev@ubuntu-server:~$ ssh -l stud9 edu.kurgasov.ru
The authenticity of host 'edu.kurgasov.ru (178.234.29.197)' can't be established.
ECDSA key fingerprint is SHA256:c7y8uU2/zFt5w6UuLfUeRk/OhPMih9uki+EYZVo1qik.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added 'edu.kurgasov.ru,178.234.29.197' (ECDSA) to the list of known hosts.
stud9@edu.kurgasov.ru's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

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

22 packages can be updated.
5 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Jan 17 16:40:41 2021 from 100.113.139.26
stud9@kurgasov:~$ _
```

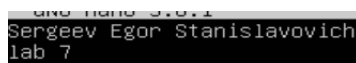
Рисунок 6 – Установление шифрованного соединения.

1.7. Вывод информации об удаленной системе

```
Last login: Sun Apr 11 18:48:41 2021 from 100.113.109.20
stud9@kurgasov:~$ uname -a
Linux kurgasov.ru 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 2021 x86_64 x86_64 x86_64
4 GNU/Linux
stud9@kurgasov:~$
```

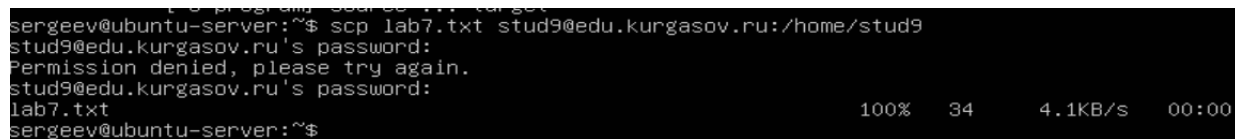
Рисунок 7 – Вывод информации об удаленной системе.

1.8. Передача файла по зашифрованному каналу




```
glibc 2.15
Sergeev Egor Stanislavovich
lab 7
```

Рисунок 8 – Содержимое файла lab7.txt.



```
sergeev@ubuntu-server:~$ scp lab7.txt stud9@edu.kurgasov.ru:/home/stud9
stud9@edu.kurgasov.ru's password:
Permission denied, please try again.
stud9@edu.kurgasov.ru's password:
lab7.txt                                100% 34      4.1KB/s   00:00
sergeev@ubuntu-server:~$
```

Рисунок 9 – Передача файла по зашифрованному каналу.



```
stud9@kurgasov:~$ ls
conf lab7.txt mail tmp web
stud9@kurgasov:~$
```

Рисунок 10 – Проверка наличия копии файла.

1.9. Формирование зашифрованных ключей

```
sergeev@ubuntu-server:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/sergeev/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/sergeev/.ssh/id_rsa
Your public key has been saved in /home/sergeev/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:rsMHC/H23UdXdFurpN5nSGvKpf6yTxq06gSzQNLoUeQ sergeev@ubuntu-server
The key's randomart image is:
+----[RSA 3072]-----+
|      .o              |
|      =               +|
|      + E             .|=|
|      .+.             .o.|
|      .Soo o o .|
|      o...o= + .+|
|      . +..o.+.*++|
|      o.. o.B+Bo|
|      .o .=..*=+|
+-----[SHA256]-----+
sergeev@ubuntu-server:~$
```

Рисунок 11 – Формирование зашифрованных ключей.

1.10. Передача публичного ключа

```
sergeev@ubuntu-server:~$ ssh-copy-id -i .ssh/id_rsa.pub stud9@kurgasov.ru
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ".ssh/id_rsa.pub"
The authenticity of host 'kurgasov.ru (178.234.29.197)' can't be established.
ECDSA key fingerprint is SHA256:c7y8uU2/zFt5w6UuLfUeRk/0hPMih9uki+EY2Vo1qik.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install all the new keys
stud9@kurgasov.ru's password:
Permission denied, please try again.
stud9@kurgasov.ru's password:

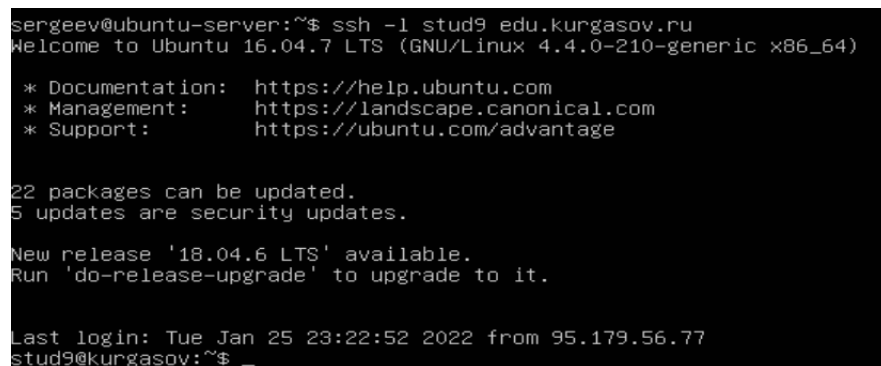
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'stud9@kurgasov.ru'"
and check to make sure that only the key(s) you wanted were added.

sergeev@ubuntu-server:~$
```

Рисунок 12 – Передача публичного ключа.

1.11. Подключение к удаленной системе



```
sergeev@ubuntu-server:~$ ssh -l stud9 edu.kurgasov.ru
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

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

22 packages can be updated.
5 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jan 25 23:22:52 2022 from 95.179.56.77
stud9@kurgasov:~$ _
```

Рисунок 13 – Подключение к удаленной системе.

1.12. Передача файла по зашифрованному каналу

```
sergeev@ubuntu-server:~$ scp lab7.txt stud9@edu.kurgasov.ru:/home/stud9
lab7.txt                                100% 34      5.3KB/s  00:00
sergeev@ubuntu-server:~$ _
```

Рисунок 14 – Передача файла по зашифрованному каналу.

1.13. Содержимое файла telnet.log

```
19:31:12.598969 IP (tos 0x10, ttl 64, id 32215, offset 0, flags [DF], proto TCP (6), length 60)
  10.0.2.15.33792 > 178.234.29.197.22: Flags [S], cksum 0xdcec (incorrect -> 0xa926), seq 9690828>
19:31:12.606337 IP (tos 0x0, ttl 64, id 35, offset 0, flags [none], proto TCP (6), length 44)
  178.234.29.197.22 > 10.0.2.15.33792: Flags [S.], cksum 0x8bae (correct), seq 1600001, ack 96908>
19:31:12.606391 IP (tos 0x10, ttl 64, id 32216, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.33792 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0xa87a), ack 1, win >
19:31:12.620152 IP (tos 0x0, ttl 64, id 36, offset 0, flags [none], proto TCP (6), length 82)
  178.234.29.197.22 > 10.0.2.15.33792: Flags [P.], cksum 0x7ce4 (correct), seq 1:43, ack 1, win 6>
19:31:12.620187 IP (tos 0x10, ttl 64, id 32217, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.33792 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0xa87a), ack 43, win>
19:31:12.626421 IP (tos 0x0, ttl 64, id 38, offset 0, flags [none], proto TCP (6), length 40)
  178.234.29.197.22 > 10.0.2.15.33792: Flags [F.], cksum 0xa340 (correct), seq 43, ack 1, win 655>
19:31:12.626586 IP (tos 0x10, ttl 64, id 32218, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.33792 > 178.234.29.197.22: Flags [F.], cksum 0xdcd8 (incorrect -> 0xa879), seq 1, ack>
19:31:12.629763 IP (tos 0x0, ttl 64, id 39, offset 0, flags [none], proto TCP (6), length 40)
  178.234.29.197.22 > 10.0.2.15.33792: Flags [.], cksum 0xa33f (correct), ack 2, win 65535, lengt>
19:35:16.690059 IP (tos 0x10, ttl 64, id 43266, offset 0, flags [DF], proto TCP (6), length 60)
  10.0.2.15.33794 > 178.234.29.197.22: Flags [S], cksum 0xdcec (incorrect -> 0xcd00), seq 7733386>
19:35:16.709145 IP (tos 0x0, ttl 64, id 40, offset 0, flags [none], proto TCP (6), length 44)
  178.234.29.197.22 > 10.0.2.15.33794: Flags [S.], cksum 0x8009 (correct), seq 18240001, ack 7733>
19:35:16.709201 IP (tos 0x10, ttl 64, id 43267, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.33794 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0x9cd5), ack 1, win >
19:35:16.723411 IP (tos 0x0, ttl 64, id 41, offset 0, flags [none], proto TCP (6), length 82)
  178.234.29.197.22 > 10.0.2.15.33794: Flags [P.], cksum 0x713f (correct), seq 1:43, ack 1, win 6>
19:35:16.723439 IP (tos 0x10, ttl 64, id 43268, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.2.15.33794 > 178.234.29.197.22: Flags [.], cksum 0xdcd8 (incorrect -> 0x9cd5), ack 43, win>
19:35:20.641833 IP (tos 0x10, ttl 64, id 43269, offset 0, flags [DF], proto TCP (6), length 42)
  10.0.2.15.33794 > 178.234.29.197.22: Flags [P.], cksum 0xdcd8 (incorrect -> 0x8fc1), seq 1:3, a>
19:35:20.642117 IP (tos 0x0, ttl 64, id 42, offset 0, flags [none], proto TCP (6), length 40)
  178.234.29.197.22 > 10.0.2.15.33794: Flags [.], cksum 0x979a (correct), ack 3, win 65535, lengt>
19:35:20.647839 IP (tos 0x0, ttl 64, id 43, offset 0, flags [none], proto TCP (6), length 59)
  178.234.29.197.22 > 10.0.2.15.33794: Flags [P.], cksum 0x1af5 (correct), seq 43:62, ack 3, win >
[ Read 64 lines ]
```

Рисунок 15 – Содержимое файла telnet.log.

Вывод

В результате выполнения лабораторной работы я получил знания по программному обеспечению удаленного доступа к распределённым системам обработки данных.