

Липецкий государственный технический университет

Факультет автоматизации и информатики

Автоматизированные системы управления

ЛАБОРАТОРНАЯ РАБОТА №6

по курсу ДПО Интаро - Linux

«Работа с SSH»

Студент

Митина М. В.

Группа ПИ-20-1

Руководитель
доц.

Кургасов В.В.

Липецк 2022 г.

Цель работы

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

IP: 10.0.0.101

Порт: 22

Логин: mystudent

Пароль: 12345

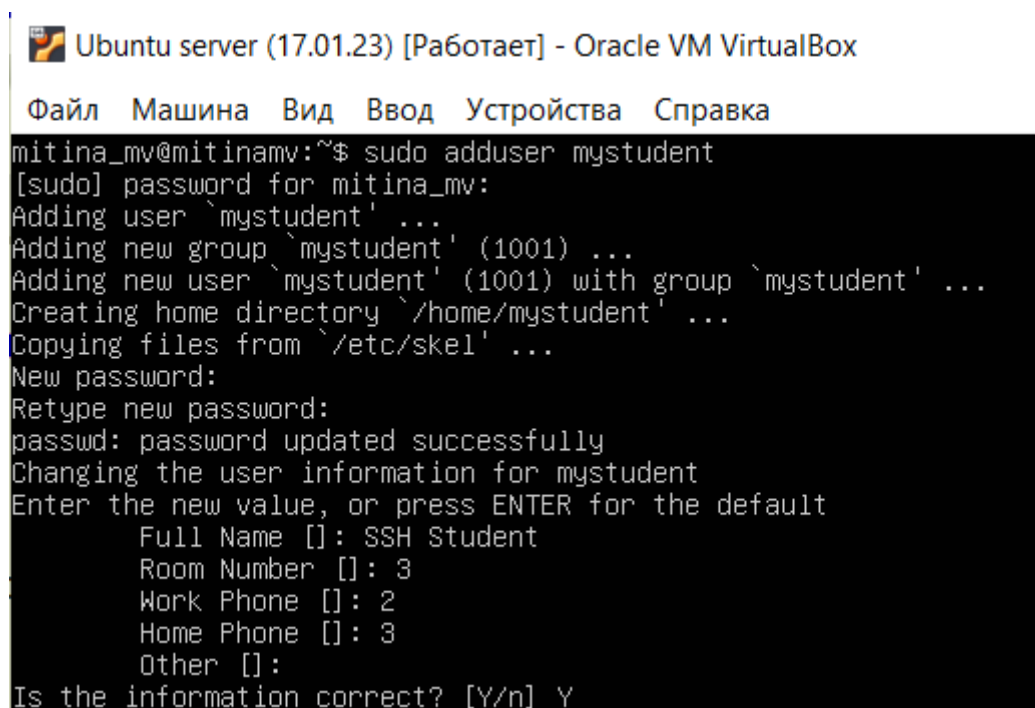
Оглавление

Ход работы	4
Настройка рабочего окружения	4
Запуск анализатора трафика tcpdump	5
Установление шифрованного соединения с удаленным сервером.....	6
Передача файла по шифрованному каналу	7
Формирование зашифрованных ключей.....	8
Содержимое файлов telnet.log и ssh.log	9
Вывод.....	11
Контрольные вопросы	12

Ход работы

Настройка рабочего окружения

Так как нам не выделили подключения, я решила использовать одну виртуальную машину в качестве терминала для подключения, а вторую – как удаленный сервер. Сервером выбрана машина под Ubuntu, оставшаяся с ЛР5. Там создаю пользователя.



```
Ubuntu server (17.01.23) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
mitina_mv@mitinamv:~$ sudo adduser mystudent
[sudo] password for mitina_mv:
Adding user `mystudent' ...
Adding new group `mystudent' (1001) ...
Adding new user `mystudent' (1001) with group `mystudent' ...
Creating home directory `/home/mystudent' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for mystudent
Enter the new value, or press ENTER for the default
    Full Name []: SSH Student
    Room Number []: 3
    Work Phone []: 2
    Home Phone []: 3
    Other []:
Is the information correct? [Y/n] Y
```

Рисунок 1 – Создаю пользователя на машине с Ubuntu.

Далее на Ubuntu нужно поставить пакеты net-tools и nc. Первый нужен для работы команды ifconfig, которая поможет узнать ip нашей машины-сервера. Вторая понадобится чуть позже в ходе выполнения ЛР.

Из ЛР5 я знаю, как пробрасывать порты из ВМ на основную машину, но так как планируется связать две машины между собой, вариант с NAT уже не подойдет. Для обеих машин в настройках сети выбираем вариант «Сетевой мост» - и теперь можно будет с одной машины подключиться на другую, но нужно знать ip сервера для подключения. Узнаю его:

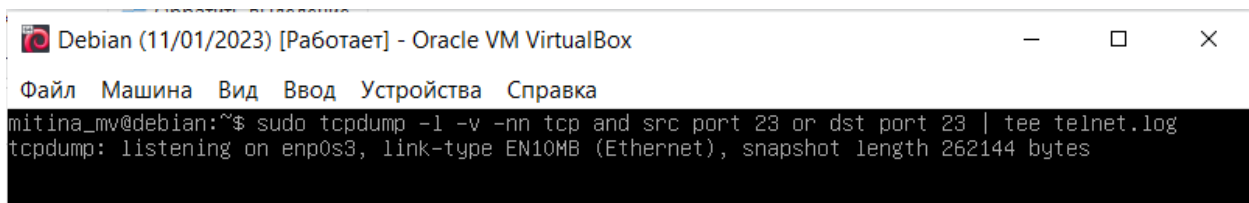
```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.101 netmask 255.0.0.0 broadcast 10.255.255.255
    inet6 fe80::a00:27ff:fe05:f3f7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:05:f3:f7 txqueuelen 1000 (Ethernet)
    RX packets 222 bytes 253615 (253.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 145 bytes 13476 (13.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рисунок 2 – запоминаем ip машины-сервера.

Порт доступа будет по умолчанию 22. Его можно изменить в конфигах ssh, но я не буду) Все готово, можно выполнять лабораторную работу.

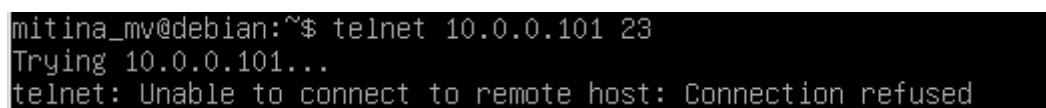
Запуск анализатора трафика tcpdump

Перед началом на нашу основную VM – Debian – нужно поставить еще несколько пакетов: tcpdump, tmux. Теперь выполняем tmux – открывается терминальный мультиплексор, который позволяет нам в одном терминале запускать несколько терминальных сессий.



```
mitina_mv@debian:~$ sudo tcpdump -l -v -nn tcp and src port 23 or dst port 23 | tee telnet.log
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

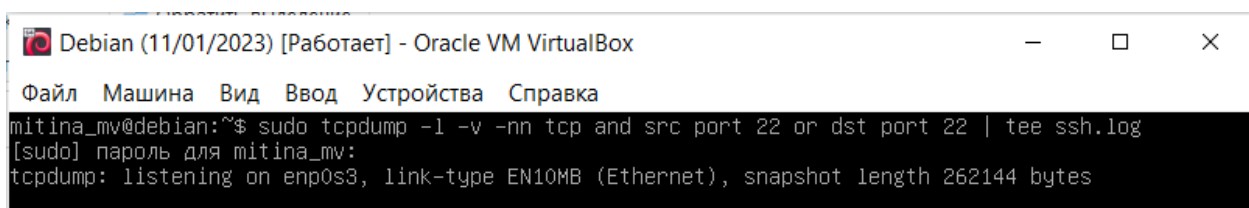
Рисунок 3 – запускаем отслеживание обращений по 23 порту



```
mitina_mv@debian:~$ telnet 10.0.0.101 23
Trying 10.0.0.101...
telnet: Unable to connect to remote host: Connection refused
```

Рисунок 4 – Стучимся к нашему ip по 23 порту - неудачно

Сочетанием Ctrl+C прерву отслеживание 23 порта, и начну отслеживать 22:



```
mitina_mv@debian:~$ sudo tcpdump -l -v -nn tcp and src port 22 or dst port 22 | tee ssh.log
[sudo] пароль для mitina_mv:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

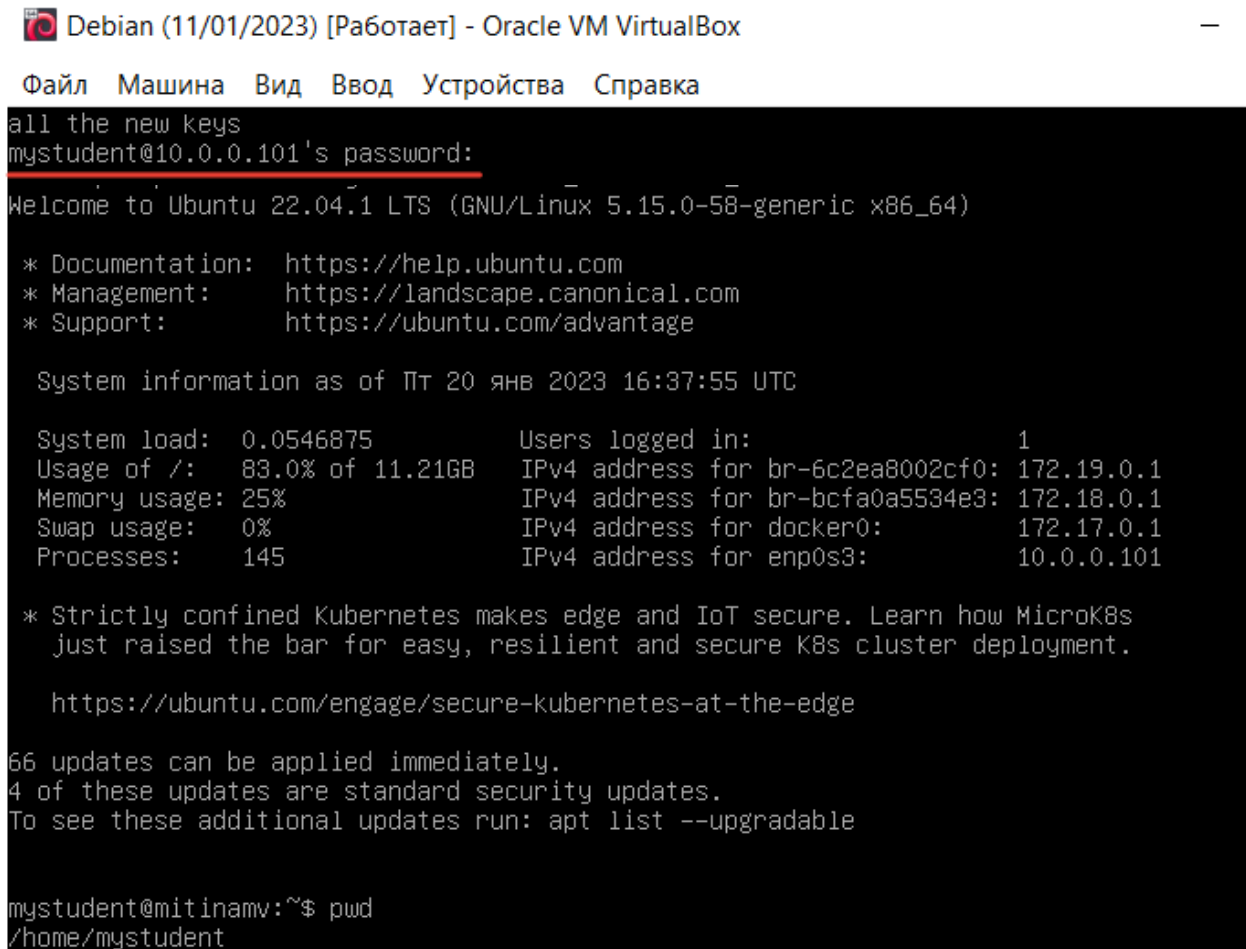
Рисунок 5 – запускаем отслеживание обращений по 22 порту

```
mitina_mv@debian:~$ telnet 10.0.0.101 22
Trying 10.0.0.101...
Connected to 10.0.0.101.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1
```

Рисунок 6 – обращаемся к 22 порту по ip – успех

Установка шифрованного соединения с удаленным сервером

Выполню ssh mystudent@10.0.0.101:



```
Debian (11/01/2023) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
all the new keys
mystudent@10.0.0.101's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-58-generic x86_64)

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

System information as of Пт 20 янв 2023 16:37:55 UTC

System load: 0.0546875      Users logged in:      1
Usage of /: 83.0% of 11.21GB IPv4 address for br-6c2ea8002cf0: 172.19.0.1
Memory usage: 25%          IPv4 address for br-bcfa0a5534e3: 172.18.0.1
Swap usage: 0%             IPv4 address for docker0:      172.17.0.1
Processes: 145             IPv4 address for enp0s3:      10.0.0.101

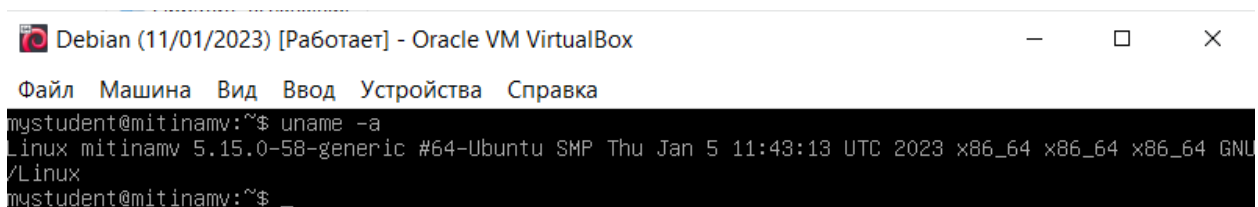
 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

66 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

mystudent@mitinamv:~$ pwd
/home/mystudent
```

Рисунок 7 – подключение с использованием пароля



```
Debian (11/01/2023) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
mystudent@mitinamv:~$ uname -a
Linux mitinamv 5.15.0-58-generic #64-Ubuntu SMP Thu Jan 5 11:43:13 UTC 2023 x86_64 x86_64 x86_64 GNU
/Linux
mystudent@mitinamv:~$ _
```

Рисунок 8 – смотрим информацию об удаленном сервере

Передача файла по зашифрованному каналу

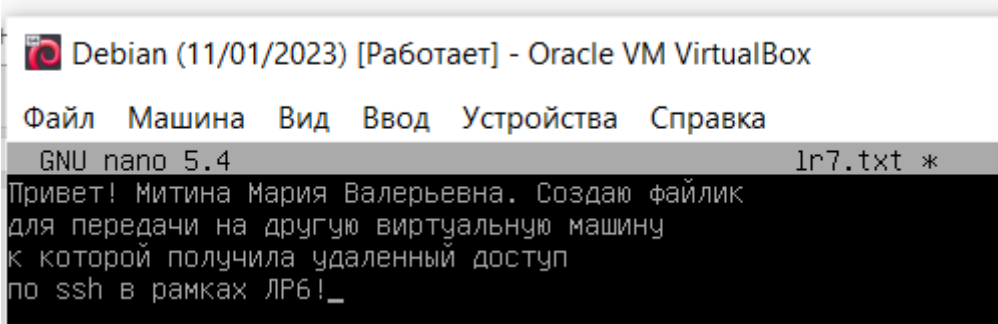


Рисунок 9 – Создаем файл для передачи по ssh

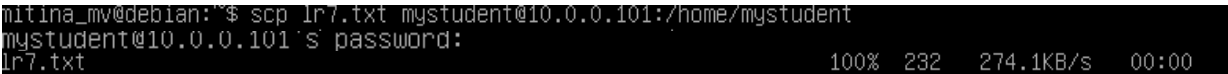


Рисунок 10 – Передача файла (запрашивается пароль)

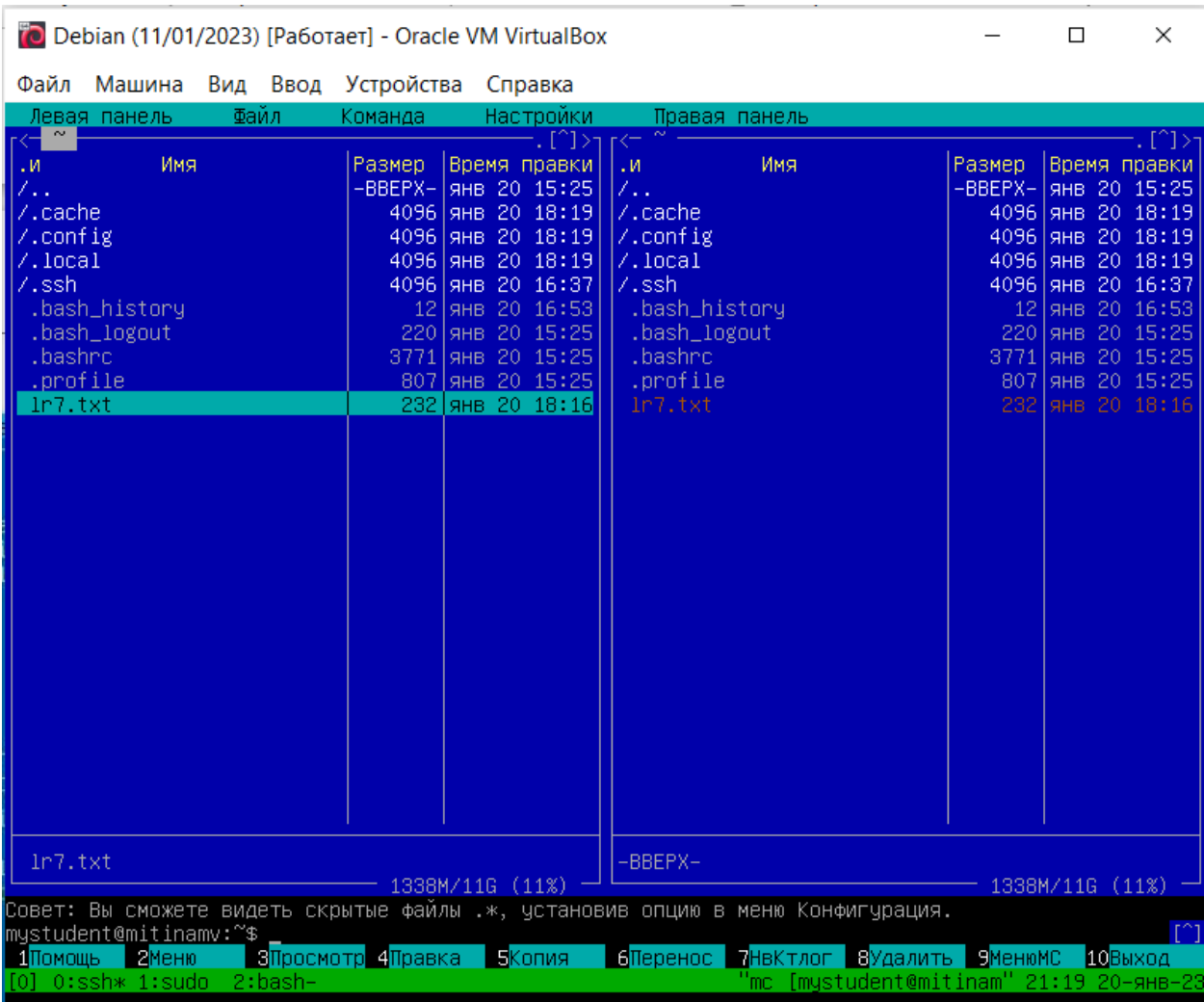


Рисунок 11 – Проверка наличия файла на удаленном сервере командой mc

Формирование зашифрованных ключей

На моей основной машине – Debian – создаем ssh-ключ командой `ssh-keygen`.

```
mitina_mv@debian:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/mitina_mv/.ssh/id_rsa): y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in y
Your public key has been saved in y.pub
The key fingerprint is:
SHA256:z7vfYukrCBoHEFBuU/qU42DZ5h+9LWl3IOfjsS/R85I mitina_mv@debian
The key's randomart image is:
+---[RSA 3072]-----+
|.++O.
|  .  .
|  ..
|  ..
|  .. S .
|  +..O..O+ O
|  = *+...*+O =
|  . B.. .O*+E..
|  +....+*@=+.
+-----[SHA256]-----+
```

Рисунок 12 – Создание ключа

Затем нужно передать ключ на удаленный сервер командой `ssh-copy-id`:

```
mitina_mv@debian:~$ ssh-copy-id mystudent@10.0.0.101
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/mitina_mv/.ssh/id_rsa.pub"
The authenticity of host '10.0.0.101 (10.0.0.101)' can't be established.
ECDSA key fingerprint is SHA256:0E1y7v7Lt9njxaTQAPJmcbfrS9PSRsD62kTgQKEFfmk.
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
mystudent@10.0.0.101's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'mystudent@10.0.0.101'"
and check to make sure that only the key(s) you wanted were added.
```

Рисунок 13 – Передача публичного ключа на сервер

Теперь снова авторизуемся на сервере по ssh. При создании ключа я добавила пароль, так что сервер попросит пароль для применения ключа:


```

mitina_mv@debian:~$ ssh mystudent@10.0.0.101
Enter passphrase for key '/home/mitina_mv/.ssh/id_rsa':
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-58-generic x86_64)

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

System information as of Пт 20 янв 2023 20:43:14 UTC

System load:  0.0                       Users logged in: 1
Usage of /:   83.1% of 11.21GB          IPv4 address for br-6c2ea8002cf0: 172.19.0.1
Memory usage: 27%                     IPv4 address for br-bcfa0a5534e3: 172.18.0.1
Swap usage:   0%                       IPv4 address for docker0: 172.17.0.1
Processes:   144                       IPv4 address for enp0s3: 10.0.0.101

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

66 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Fri Jan 20 20:22:50 2023 from 10.0.0.103

```

Рисунок 14 – авторизация по ssh с ключом (пароль пользователя не понадобился)

Попробуем теперь передать файл:

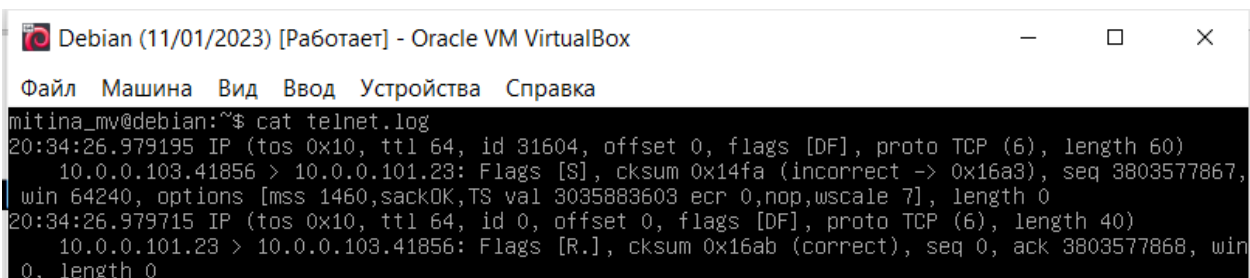
```

mitina_mv@debian:~$ scp lr7.txt mystudent@10.0.0.101:/home/mystudent
Enter passphrase for key '/home/mitina_mv/.ssh/id_rsa':
lr7.txt                                     100% 232   274.1KB/s   00:00

```

Рисунок 15 – передача файла (пароль пользователя не понадобился, но вводился пароль для применения ключа ssh)

Содержимое файлов telnet.log и ssh.log



```

mitina_mv@debian:~$ cat telnet.log
20:34:26.979195 IP (tos 0x10, ttl 64, id 31604, offset 0, flags [DF], proto TCP (6), length 60)
  10.0.0.103.41856 > 10.0.0.101.23: Flags [S], cksum 0x14fa (incorrect -> 0x16a3), seq 3803577867,
  win 64240, options [mss 1460,sackOK,TS val 3035883603 ecr 0,nop,wscale 7], length 0
20:34:26.979715 IP (tos 0x10, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
  10.0.0.101.23 > 10.0.0.103.41856: Flags [R.], cksum 0x16ab (correct), seq 0, ack 3803577868, win
  0, length 0

```

Рисунок 16 – Содержимое файла telnet.log

```
Debian (11/01/2023) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
21:44:58.296111 IP (tos 0x0, ttl 64, id 41721, offset 0, flags [DF], proto TCP (6), length 60)
    10.0.0.103.38992 > 10.0.0.101.22: Flags [S], cksum 0x14fa (incorrect -> 0xbc51), seq 2626623710,
    win 64240, options [mss 1460,sackOK,TS val 3040114921 ecr 0,nop,wscale 7], length 0
21:44:58.296447 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    10.0.0.101.22 > 10.0.0.103.38992: Flags [S.], cksum 0x2fc3 (correct), seq 1037561955, ack 262662
    3711, win 65160, options [mss 1460,sackOK,TS val 392119115 ecr 3040114921,nop,wscale 7], length 0
21:44:58.296481 IP (tos 0x0, ttl 64, id 41722, offset 0, flags [DF], proto TCP (6), length 52)
    10.0.0.103.38992 > 10.0.0.101.22: Flags [.] , cksum 0x14f2 (incorrect -> 0x5b22), ack 1, win 502,
    options [nop,nop,TS val 3040114921 ecr 392119115], length 0
21:44:58.296984 IP (tos 0x0, ttl 64, id 41723, offset 0, flags [DF], proto TCP (6), length 92)
    10.0.0.103.38992 > 10.0.0.101.22: Flags [P.], cksum 0x151a (incorrect -> 0xf51f), seq 1:41, ack
    1, win 502, options [nop,nop,TS val 3040114922 ecr 392119115], length 40: SSH: SSH-2.0-OpenSSH_8.4p1
    Debian-5+deb11u1
21:44:58.297451 IP (tos 0x0, ttl 64, id 56355, offset 0, flags [DF], proto TCP (6), length 52)
    10.0.0.101.22 > 10.0.0.103.38992: Flags [.] , cksum 0x5af1 (correct), ack 41, win 509, options [r
    nop,nop,TS val 392119116 ecr 3040114922], length 0
21:44:58.307297 IP (tos 0x0, ttl 64, id 56356, offset 0, flags [DF], proto TCP (6), length 93)
    10.0.0.101.22 > 10.0.0.103.38992: Flags [P.], cksum 0x328f (correct), seq 1:42, ack 41, win 509,
    options [nop,nop,TS val 392119126 ecr 3040114922], length 41: SSH: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ub
    untu0.1
21:44:58.307330 IP (tos 0x0, ttl 64, id 41724, offset 0, flags [DF], proto TCP (6), length 52)
    10.0.0.103.38992 > 10.0.0.101.22: Flags [.] , cksum 0x14f2 (incorrect -> 0x5abb), ack 42, win 502
    , options [nop,nop,TS val 3040114932 ecr 392119126], length 0
21:44:58.307927 IP (tos 0x0, ttl 64, id 41725, offset 0, flags [DF], proto TCP (6), length 1564)
    10.0.0.103.38992 > 10.0.0.101.22: Flags [P.], cksum 0x1ada (incorrect -> 0x760f), seq 41:1553, a
    ck 42, win 502, options [nop,nop,TS val 3040114933 ecr 392119126], length 1512
21:44:58.308931 IP (tos 0x0, ttl 64, id 56357, offset 0, flags [DF], proto TCP (6), length 1132)
    10.0.0.101.22 > 10.0.0.103.38992: Flags [P.], cksum 0x3ed4 (correct), seq 42:1122, ack 1553, win
    499, options [nop,nop,TS val 392119128 ecr 3040114933], length 1080
21:44:58.311233 IP (tos 0x0, ttl 64, id 41727, offset 0, flags [DF], proto TCP (6), length 100)
    10.0.0.103.38992 > 10.0.0.101.22: Flags [P.], cksum 0x1522 (incorrect -> 0x7471), seq 1553:1601,
    ack 1122, win 501, options [nop,nop,TS val 3040114936 ecr 392119128], length 48
21:44:58.316553 IP (tos 0x0, ttl 64, id 56358, offset 0, flags [DF], proto TCP (6), length 648)
    10.0.0.101.22 > 10.0.0.103.38992: Flags [P.], cksum 0xfab0 (correct), seq 1122:1718, ack 1601, w
    in 501, options [nop,nop,TS val 392119135 ecr 3040114936], length 596
ssh.log
[0] 0:less* 1:sudo~ 2:bash "mc [mystudent@mitinam" 21:46 20-январь-23
```

Рисунок 17 – Содержимое файла ssh.log

Вывод

В ходе выполнения лабораторной работы я научилась подключаться по ssh, генерировать ключи для доступа к удалённому серверу без использования пароля и передавать файлы.

Контрольные вопросы

1) Определите основные цели и задачи решаемые с помощью ПО удаленного доступа?

Удаленный доступ – это технология, позволяющая управлять одним устройством с другого по сети. Такой подход позволяет проще и удобнее решать множество производственных задач:

- решение технических проблем. Например, имеем несколько офисов по стране и один отдел тех. поддержки в головном офисе. Этот отдел может поддерживать все компьютеры компании с помощью удаленного доступа.
- управление сервером. Разработчики и тестировщики могут использовать арендованные сервера и иметь к ним удаленный доступ, чтобы разрабатывать и тестировать системы.
- совместная работа из разных городов.

2) Выделите отличительные особенности между режимами работы удаленного доступа по протоколам TELNET и SSH?

- SSH более защищен, чем TELNET.
- оба используют стандарт TCP, для SSH 22 порт по умолчанию, а для TELNET 23.
- SSH отправляет все данные в зашифрованном формате, а TELNET отправляет данные в виде обычного текста.
- SSH использует шифрование с открытым ключом, а TELNET не использует механизмов аутентификации. Поэтому SSH подходит для общедоступных сетей, а TELNET – для частных.

3) Опишите способы установления соединения при использовании протокола SSH? Охарактеризуйте положительные и отрицательные аспекты приведенных методов.

SSH (Secure Shell) – зашифрованный протокол, используемый для удаленного доступа. В ходе выполнения ЛР мы попробовали два способа авторизации по SSH: с использованием пароля пользователя и с использованием ssh-ключа. При создании ключа можно задать пароль на его использование, и тогда авторизация станет еще безопаснее.

Для аутентификации по ssh-ключу мы на своем компьютере создаем ключ, состоящий из открытого и закрытого ключа. Открытый передается на ту машину, удаленный доступ к которой нам нужно получить. Закрытый остается на стороне клиента и не должен быть доступен кому-то еще (в этом помогает и пароль, который можно задать при создании ключа). Открытый ключ используется для шифрования сообщений, которые можно расшифровать только закрытым ключом.

4) Основываясь на заданиях лабораторной работы, приведите практический пример использования систем удаленного доступа?

Доступ к удаленному серверу для передачи файлов и ведения разработки.

5) Перечислите распространенные сетевые службы, основанные на использовании шифрованного соединения по протоколу SSH? Приведите пример использования службы передачи файлов по безопасному туннелю?

Распространенные сетевые службы, основанные на использовании шифрованного соединения по протоколу SSH: OpenSSH, PuTTY/KiTTY, SecureCRT, Xshell. Службы передачи файлов по безопасному туннелю можно использовать для передачи паролей

6) Что такое ключ ssh? В чем преимущество их использования?

SSH-ключ – это последовательность символов, представляет собой пару ключей – открытый и закрытый. Мы знаем, что для логинов по-хорошему нужно придумывать разные пароли. Записывать их равносильно открыть злоумышленнику дверь, а запоминать – целая проблема. Кроме того, пароли

обычно имеют небольшую длину. Если учитывать вычислительные мощности, нет никаких проблем подобрать пароли средней длины в 7-12 символов. Из дискретной математики мы знаем, что количество комбинаций увеличивается с ростом алфавита либо длины комбинации. SSH ключ очень длинный, поэтому подобрать его намного труднее. Это повышает безопасность. Кроме того, ключи удобно использовать в скриптах, с помощью которых администраторы автоматизируют различные рутинные операции: установку обновлений, создание архивных копий, конфигурирование систем и сервисов. Это особенно востребовано из-за широкого распространения Agile-разработки и практик DevOps.

7) Как сгенерировать ключи ssh в разных ОС?

Для работы с SSH-ключами используются утилиты, входящие в оболочку OpenSSH. Они работают под Linux, Windows и MacOS. Для Linux и Windows для генерации ключа отработает команда `ssh-keygen`. Еще ей можно указать параметр `-t` и после указать тип создаваемого ключа (алгоритм шифрования определяет тип).

8) Возможно ли из «секретного» ключа сгенерировать «публичный» и/или наоборот?

Все зависит от алгоритма. Закрытый и открытый ключ генерируются вместе. Закрытый ключ RSA хранит поля открытого ключа, так как это полезно для оптимизированной реализации. В то же время для RSA нет возможности сгенерировать закрытый ключ из открытого, а открытый из закрытого – можно. Во многих алгоритмах просто нет такого требования как «невозможность сгенерировать один ключ из другого», поэтому все алгоритмы дают разную степень безопасности. Получить открытый ключ из закрытого не так страшно – открытым ключам сообщения шифруются, а расшифровываются закрытым, поэтому важно хранить закрытый ключ.

9) Будут ли отличаться пары ключей, сгенерированные на одном ПК несколько раз с исходными условиями (наличие/отсутствие пароля на «секретный» ключ и т.п.)

Практические исследования на ВМ для ответа на этот вопрос показали, что да, пары ключей меняются:

```
mitina_mv@debian:~$ cat ~/.ssh/id_ed25519
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1r2XktdjEAAAAACmFlczI1N11jdHIAAAAGYmNyeXB0AAAAAGAAAABAVLTBTbu
tyQI7X7o+p/RU/AAAAEAAAAAEAAAAzAAAAC3NzaC1lZDI1NTE5AAAAILfM80YBgoz044vR
7jyWdkTNNmGE4N/aL3087T0nzD2mAAAAoI7sKQ1JHxzJRVz/Q+b+9FWyHKoy/sYezU9TcD
QUBYXvp1DeI5dJnAru7WItupbpKBV0fgtA2sfeec1ApvJGnxp3CLIWyiuhzS7In3bzynfs
58hl+XeLx1ta3eNFU1RcxSJTr2xDJApV1INDcrt06CHzVePv1UPceuc4jJb/aQ79AdLRe4
vbjs1Xk8HWj2HCf4TpEfNiUNXk8bpdqg30LvM=
-----END OPENSSH PRIVATE KEY-----
```

```
mitina_mv@debian:~$ cat ~/.ssh/id_ed25519
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1r2XktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAAtzc2gtZW
QyNTUxOQAAACD1RpcqW6A09KbUaM5EX0FKo4c7VuoBEJW01GPdIi381wAAAJgBG+Q3ARvk
NwAAAAAtzc2gtZWQyNTUxOQAAACD1RpcqW6A09KbUaM5EX0FKo4c7VuoBEJW01GPdIi381w
AAAEAE60Yw0dB+j9ggNwYUegeWePDycNEMan4gSzptcj0boufVG1ypboDT0ptRozkRc4Uqj
hztW6gEQ1bTUY90iLzfXAAAAEG1pdGluYVY9tdkBkZWJpYW4BAgMEBQ==
-----END OPENSSH PRIVATE KEY-----
```

10) Перечислите доступные ключи для ssh-keygen.exe

- o - Заставляет ssh-keygen сохранять закрытые ключи, используя новый формат OpenSSH, а не более совместимый формат PEM.
- t - Указывает тип ключа для создания. Возможными значениями являются `rsa1` для версии протокола 1 и `dsa`, `ecdsa`, `ed25519` или `rsa` для версии протокола 2.
- v - Подробный режим. Заставляет ssh-keygen печатать сообщения об отладке о ее ходе. Это полезно для генерации модулей отладки.
- y - Эта опция считывает закрытый файл формата OpenSSH и печатает открытый ключ OpenSSH в стандартный вывод.
- p - Запрашивает изменение ключевой фразы файла закрытого ключа вместо создания нового закрытого ключа.

- `e` - Эта опция будет считывать закрытый или общедоступный файл ключа OpenSSH и распечатывать для стандартного вывода ключ в одном из форматов, указанных параметром `-m`.
- `i` - Этот параметр будет считывать незашифрованный файл закрытого (или открытого) ключа в формате, указанном `-m` выберите и распечатайте совместимый с OpenSSH закрытый (или открытый) ключ в стандартный вывод.

11) Можно ли использовать один «секретный» ключ доступа с разных ОС, установленных на одном ПК/на разных ПК?

Можно. Считается, что ssh-ключи не изнашиваются, поэтому их можно не менять и использовать для доступа на разные удаленные системы. Но лучше так не делать, потому что это снижает безопасность – получив один раз закрытый ключ, мы сможем получить доступ ко всем удаленным системам, которые используют пару публичного ключа этого ssh-ключа.

12) Возможно ли организовать подключение «по ключу» ssh к системе с ОС Windows, в которой запущен OpenSSH сервер?

Конечно, ведь поддержку OpenSSH для этого и ввели. Подключаться к винде и без ssh и OpenSSH можно было, но это было трудным занятием, а соединение не всегда стабильным.

13) Какие известные Вам сервисы сети Интернет позволяют организовать доступ к ресурсам посредством SSH ключей?

GitHub поддерживает авторизацию по ssh, для этого нужно создать секрет в аккаунте github и сохранить в секрете публичный ключ, а потом с машины постучаться на github – выполнить клон репозитория, пулл в него или что-то похожее.