Санкт-Петербургский политехнический университет Петра Великого
Институт компьютерных наук и кибербезопасности
Высшая школа программной инженерии

Практическая работа №1

по дисциплине «Сети и телекоммуникации»

Выполнил: Яровой В. Д.
Группа: 5130904/00104

Проверил: Медведев Б. М.

Санкт-Петербург
2024

Содержание

1 Ответы на вопросы

1.1 Вопрос 1

TODO

Что такое IP адрес, MAC адрес, маска подсети, порт

IP-адрес (Internet Protocol address) - это уникальный числовой идентификатор, присвоенный устройству (компьютеру, принтеру, маршрутизатору и т.д.) в сети, чтобы обеспечивать его идентификацию и обмен данными в сети.

MAC-адрес (Media Access Control address) - это уникальный идентификатор, присвоенный сетевому интерфейсу для обеспечения его уникальности в рамках локальной сети. Он используется на более низком уровне сетевого стека, чем IP-адрес, и обычно привязан к аппаратному оборудованию.

Маска подсети - это числовое значение, определяющее, какая часть IP-адреса относится к сети, а какая к устройству в этой сети. Она помогает разделять IP-адрес на сетевую и хост-части.

Порт - это логический номер, используемый для идентификации конкретного процесса, который обменивается данными через сеть. В контексте TCP/IP порты разделяются на три диапазона: известные порты (0-1023), зарегистрированные порты (1024-49151) и динамические порты (49152-65535).

1.2 Вопрос 2

TODO

Чем хорош и чем плох Telnet

Telnet - это протокол удаленного управления, который позволяет пользователю управлять удаленным компьютером через сеть. Однако Telnet передает данные в открытом виде, не обеспечивая шифрование, что делает его небезопасным для передачи чувствительной информации, такой как пароли. Лучше использовать безопасные альтернативы, такие как SSH.

1.3 Вопрос 3

TODO

Как можно улучшить безопасность подключения при использовании SSH

Использование ключей вместо паролей для аутентификации. Ограничение доступа через настройку файрвола и конфигурации SSH. Изменение порта SSH для усложнения атак. Отключение доступа к системе по умолчанию (парольного доступа) и использование только ключей. Регулярное обновление SSH и других компонентов системы.

1.4 Вопрос 4

TODO

Когда стоит использовать авторизацию по паролю, а когда по ключам, при подключении по SSH

Авторизация по паролю стоит использовать, когда ключи недоступны или неудобны для использования. Авторизация по ключам является более безопасным вариантом, так как предотвращает атаки на подбор паролей и обеспечивает сильную аутентификацию. Рекомендуется использовать ключи в более критичных сценариях.

2 Практические задание

2.1 Задание 1

TODO

Какую информацию можно узнать с помощью команд **ifconfig** (или ip) и **netstat**. Приведите примеры

Команды **ifconfig** (или ip) и **netstat** предоставляют информацию о сетевых интерфейсах, IP-адресах, маршрутах и открытых сетевых соединениях. В зависимости от операционной системы могут быть различия в синтаксисе команд. Ниже приведены примеры для Linux.

пример **ifconfig**:

```
br-23ef8c0ffb84: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:eb:6f:85:63  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:b0:59:9e:6d  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.14  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::c3b0:b42a:5d25:8e57  prefixlen 64  scopeid 0x20<link>
        ether ac:1f:6b:12:e4:78  txqueuelen 1000  (Ethernet)
        RX packets 204073  bytes 196777986 (187.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35868  bytes 5544923 (5.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfb300000-fb37ffff

eno2: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether ac:1f:6b:12:e4:79  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfb200000-fb27ffff

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1767  bytes 13431796 (12.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1767  bytes 13431796 (12.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1. br-23ef8c0ffb84:
   - flags=4099: Этот интерфейс поддерживает различные опции, такие как UP (включен), BROADCAST (разрешает отправку широковещательных сообщений), MULTICAST (поддерживает многоадресную рассылку).
   - mtu 1500: Максимальный размер пакета данных, который может быть передан через этот интерфейс.
   - inet 172.18.0.1: IP-адрес интерфейса.
   - netmask 255.255.0.0: Маска подсети для определения, какие биты IP-адреса относятся к сети и хост-части.
   - ether 02:42:eb:6f:85:63: MAC-адрес интерфейса.

   txqueuelen 0: Длина очереди передачи.
   - RX/TX packets, bytes: Статистика приема и передачи пакетов.
2. docker0:
   - Аналогичная информация для виртуального интерфейса, который используется Docker.
3. eno1:
   - flags=4163: UP, BROADCAST, RUNNING, MULTICAST. Интерфейс включен, поддерживает широковещательные сообщения, активен, поддерживает многоадресную рассылку.
   - inet 192.168.100.14: IP-адрес интерфейса.
   - netmask 255.255.255.0: Маска подсети.
   - ether ac:1f:6b:12:e4:78: MAC-адрес интерфейса.
   - RX/TX packets, bytes: Статистика приема и передачи пакетов.
   - inet6 fe80::c3b0:b42a:5d25:8e57: IPv6-адрес.
4. eno2:
   - Аналогичная информация для другого сетевого интерфейса.
5. lo:
   - flags=73: UP, LOOPBACK, RUNNING. Интерфейс включен, является интерфейсом обратной связи (loopback), активен.
   - inet 127.0.0.1: IP-адрес интерфейса.
   - netmask 255.0.0.0: Маска подсети.
   - inet6 ::1: IPv6-адрес.
   - RX/TX packets, bytes: Статистика приема и передачи пакетов по интерфейсу обратной связи.

пример вывода **netstat**:

```
unix  3      [ ]         STREAM     CONNECTED     64868
unix  2      [ ]         DGRAM      CONNECTED     55603
unix  3      [ ]         STREAM     CONNECTED     18069
unix  3      [ ]         STREAM     CONNECTED     19190
unix  3      [ ]         STREAM     CONNECTED     7730
unix  3      [ ]         STREAM     CONNECTED     21254
unix  3      [ ]         STREAM     CONNECTED     46646    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     10635
unix  3      [ ]         STREAM     CONNECTED     76869
unix  3      [ ]         STREAM     CONNECTED     43999
unix  3      [ ]         STREAM     CONNECTED     24434
unix  3      [ ]         STREAM     CONNECTED     3489
unix  3      [ ]         STREAM     CONNECTED     22631    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     13752
unix  3      [ ]         STREAM     CONNECTED     68000
unix  3      [ ]         SEQPACKET  CONNECTED     13237
unix  3      [ ]         STREAM     CONNECTED     18032
```

```
unix  3      [ ]         STREAM     CONNECTED     73042
unix  3      [ ]         STREAM     CONNECTED     12101    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     17768
unix  3      [ ]         SEQPACKET  CONNECTED     21047
unix  3      [ ]         STREAM     CONNECTED     11537
unix  3      [ ]         STREAM     CONNECTED     86103
unix  3      [ ]         STREAM     CONNECTED     7843     /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     138377
unix  3      [ ]         STREAM     CONNECTED     53052
```

1. Столбцы:
   - Proto: Протокол (в данном случае, «unix» для сокетов Unix).
   - Recv-Q и Send-Q: Длина очереди приема и отправки данных.
   - Локальный адрес и состояние: Локальный адрес сокета и его текущее состояние.
   - Удаленный адрес: Удаленный адрес (если соединение удаленное).
2. Строки:
   - CONNECTED: Состояние, в котором соединение установлено.
   - DGRAM: Датаграммный сокет (без установления соединения).
   - SEQPACKET: Последовательный пакет (для надежной и упорядоченной передачи данных).
3. Примеры строк из вывода:
   - unix 3 [ ] STREAM CONNECTED 64868: Сокет Unix в состоянии CONNECTED с локальным адресом. Номер сокета 64868.
   - unix 2 [ ] DGRAM CONNECTED 55603: Датаграммный сокет (без установления соединения) с номером 55603.
   - unix 3 [ ] SEQPACKET CONNECTED 13237: Сокет Unix типа SEQPACKET в состоянии CONNECTED с номером 13237.
   - unix 3 [ ] STREAM CONNECTED 46646 /run/dbus/system_bus_socket: Сокет Unix в состоянии CONNECTED с путем к файлу (здесь это файл сокета системной шины D-Bus)

2.2 Задание 2

TODO

Посмотрите файлы /etc/services, /etc/protocols, расскажите на каких портах работают основные сервисы (ssh, ftp, http, smtp и др.)

etc/services:

```
ftp                 21/tcp
ftp                 21/udp
ftp                 21/sctp
...
ssh                 22/tcp
ssh                 22/udp
ssh                 22/sctp
...
http                80/tcp
http                80/udp
http                80/sctp
...
smtp                25/tcp
smtp                25/udp
```

```
...
https            443/tcp
https            443/udp
https            443/sctp
```

etc/protocols:

```
# Full data: /usr/share/iana-etc/protocol-numbers.iana

hopopt          0 HOPOPT
icmp            1 ICMP
igmp            2 IGMP
ggp             3 GGP
ipv4            4 IPv4
st              5 ST
tcp             6 TCP
cbt             7 CBT
egp             8 EGP
igp             9 IGP
bbn-rcc-mon    10 BBN-RCC-MON
nvp-ii         11 NVP-II
pup            12 PUP
emcon          14 EMCON
xnet           15 XNET
...
```

2.3 Задание 3

TODO

Настройте подключение по ssh к какому-либо серверу (в крайнем случае к localhost) с использованием ключей шифрования.

В рамках задания будем подключаться к виртуальной машине
Создаем ключи:

```
ssh-keygen -t rsa
```

Проверяем их наличие:

```
-rw------- 1 vadim vadim 2602 фев 17 12:29 netlab
-rw-r--r-- 1 vadim vadim  573 фев 17 12:29 netlab.pub
```

включаем ssh на сервере:

```
sudo systemctl enable sshd service
Created symlink /etc/systemd/system/multi-user.target.wants/sshd.service → /usr/lib/
systemd/system/sshd.service.
sudo systemctl start sshd.service
sudo systemctl status sshd.service
● sshd.service - OpenSSH Daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: disabled)
     Active: active (running) since Sat 2024-02-17 12:35:21 MSK; 3s ago
```

```
   Main PID: 17516 (sshd)
      Tasks: 1 (limit: 4669)
     Memory: 2.1M (peak: 2.3M)
        CPU: 21ms
     CGroup: /system.slice/sshd.service
             └─17516 "sshd: /usr/bin/sshd -D [listener] 0 of 10-100 startups"

фев 17 12:35:21 vadim-virtualbox systemd[1]: Started OpenSSH Daemon.
фев 17 12:35:21 vadim-virtualbox sshd[17516]: Server listening on 0.0.0.0 port 22.
фев 17 12:35:21 vadim-virtualbox sshd[17516]: Server listening on :: port 22.
```

Копируем ключи на сервер и вводим пароль:

```
ssh-copy-id vadim@192.168.100.15
```

Результат подключения:

```
[vadim@vadim-virtualbox ~]$
```

Если ssh-copy-id недоступен, вы можете скопировать содержимое публичного ключа вручную и добавить его в файл /.ssh/authorized_keys на сервере.

Подключаемся к серверу с помощью ключа:

```
ssh vadim@192.168.100.15
```

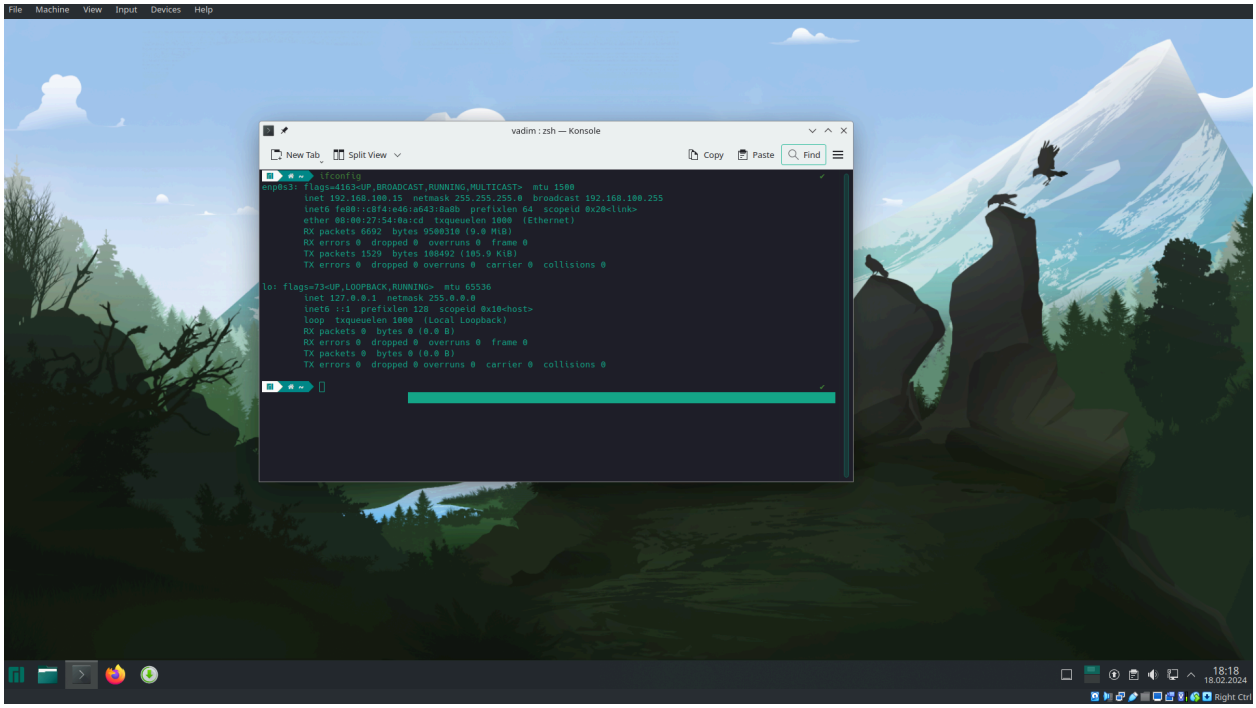

Рис. 1. Узнаем IP адрес

Рис. 2. Подключаемся

Отключаем аутентификацию по паролю в файле конфигурации SSH (/etc/ssh/sshd_config на сервере)

```
PasswordAuthentication no
```

Перезапускаем службу SSH на сервере

2.4 Задание 4

Настройка параметров подключения по SSH может улучшить безопасность и эффективность соединения. Ниже приведены некоторые параметры конфигурации SSH, которые могут быть полезны в различных сценариях:

1. Порт SSH:
   - Опция: Port
   - Пример: Port 2222
   - Когда использовать: Изменение порта SSH может обеспечить дополнительный уровень безопасности, уменьшив количество неудачных попыток входа, но также может усложнить подключение. Используйте это, если хотите уменьшить количество неудачных попыток входа.
2. Отключение аутентификации по паролю:
   - Опция: PasswordAuthentication no
   - Когда использовать: Используйте это, если хотите разрешить только аутентификацию по ключам, усиливая безопасность.
3. Ограничение пользователя:
   - Опция: AllowUsers username
   - Пример: AllowUsers vadim yarovoy
   - Когда использовать: Ограничьте доступ только определенным пользователям, что полезно для управления доступом.
4. Ограничение IP-адресов:
   - Опция: AllowUsers username@ip_address
   - Пример: AllowUsers yarovoy@192.168.1.2
   - Когда использовать: Ограничьте доступ по определенным IP-адресам, уменьшая поверхность атаки.
5. Использование только протокола SSHv2:
   - Опция: Protocol 2
   - Когда использовать: Отключите устаревший протокол SSHv1 в пользу более безопасного SSHv2.
6. Отключение удаленного входа для root:
   - Опция: PermitRootLogin no
   - Когда использовать: Отключите возможность входа в систему непосредственно под пользователем root для усиления безопасности.

Для внесения этих изменений, отредактируем файл /etc/ssh/sshd_config на сервере. После внесения изменений, перезапускаем службу SSH для применения новых настроек.

3 Вывод

Были использованы и проанализированы базовые сетевые команды и файлы конфигурации. Настроено безопасное подключение по SSH с использованием ключей, а также рассмотрены меры безопасности и различные настройки для улучшения безопасности подключений. Получены практические навыки работы с основными сетевыми инструментами и сервисами.