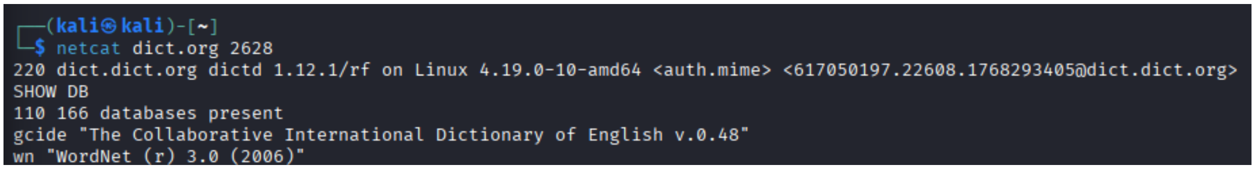
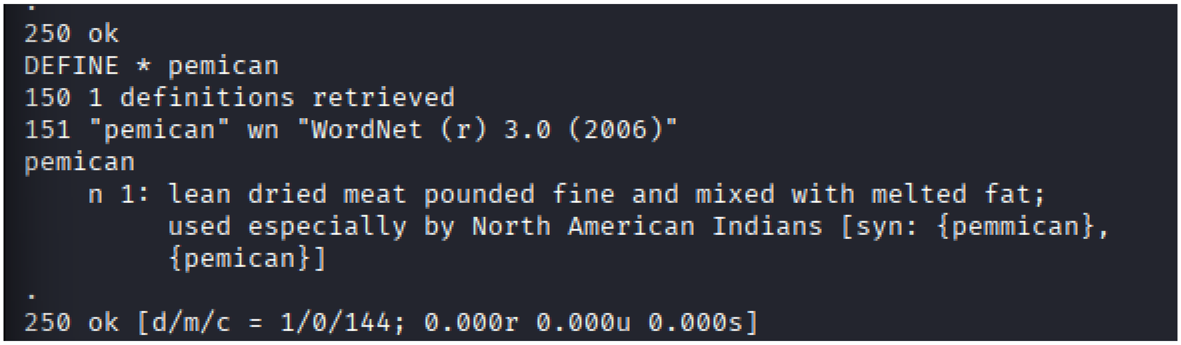
Exercise 1

1. 166 Databases presents



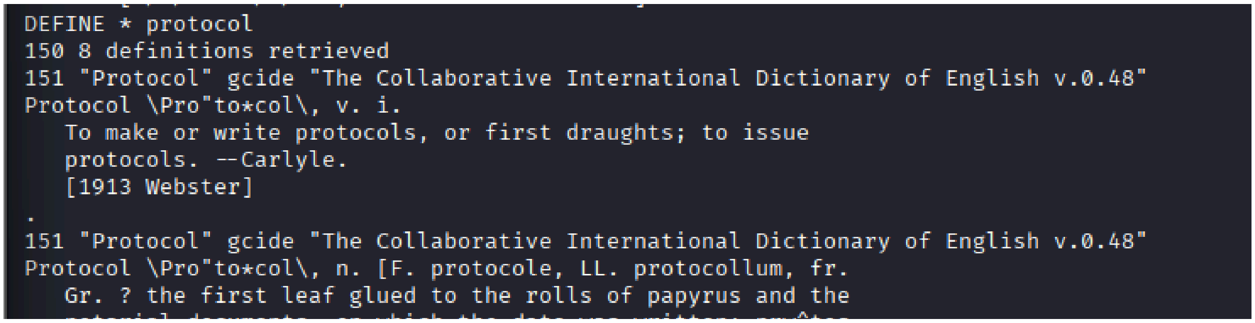
```
┌──(kali㉿kali)-[~]
└─$ netcat dict.org 2628
220 dict.dict.org dictd 1.12.1/rf on Linux 4.19.0-10-amd64 <auth.mime> <617050197.22608.1768293405@dict.dict.org>
SHOW DB
110 166 databases present
gcide "The Collaborative International Dictionary of English v.0.48"
wn "WordNet (r) 3.0 (2006)"
```

2. DEFINE * pemican



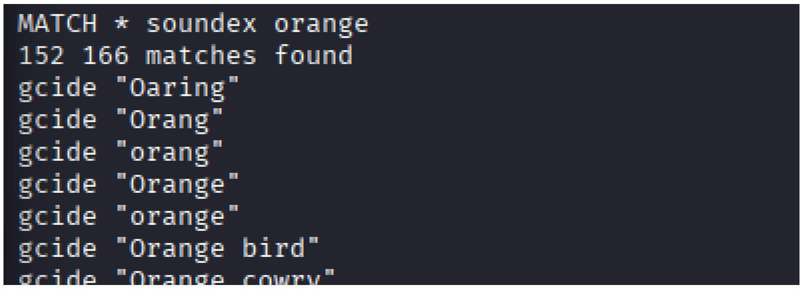
```
.
250 ok
DEFINE * pemican
150 1 definitions retrieved
151 "pemican" wn "WordNet (r) 3.0 (2006)"
pemican
    n 1: lean dried meat pounded fine and mixed with melted fat;
         used especially by North American Indians [syn: {pemmican},
         {pemican}]
.
250 ok [d/m/c = 1/0/144; 0.000r 0.000u 0.000s]
```

3. 8 dictionaries



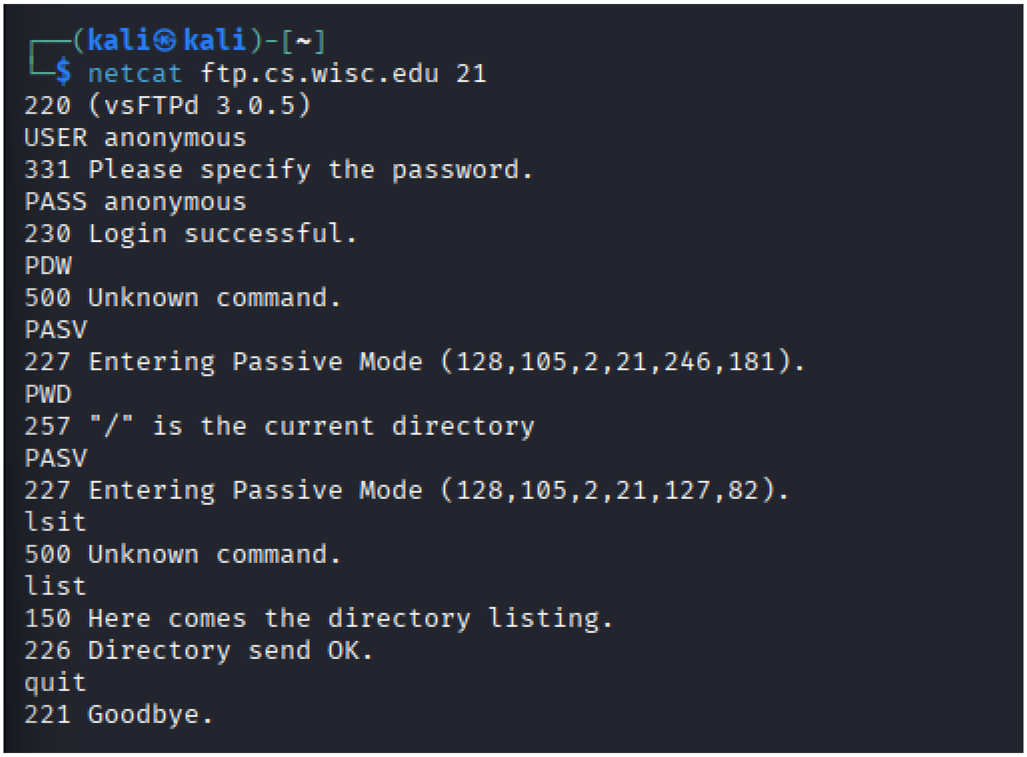
```
DEFINE * protocol
150 8 definitions retrieved
151 "Protocol" gcide "The Collaborative International Dictionary of English v.0.48"
Protocol \Pro"to*col\, v. i.
   To make or write protocols, or first draughts; to issue
   protocols. --Carlyle.
   [1913 Webster]
.
151 "Protocol" gcide "The Collaborative International Dictionary of English v.0.48"
Protocol \Pro"to*col\, n. [F. protocole, LL. protocollum, fr.
   Gr. ? the first leaf glued to the rolls of papyrus and the
```

4. MATCH * soundex orange

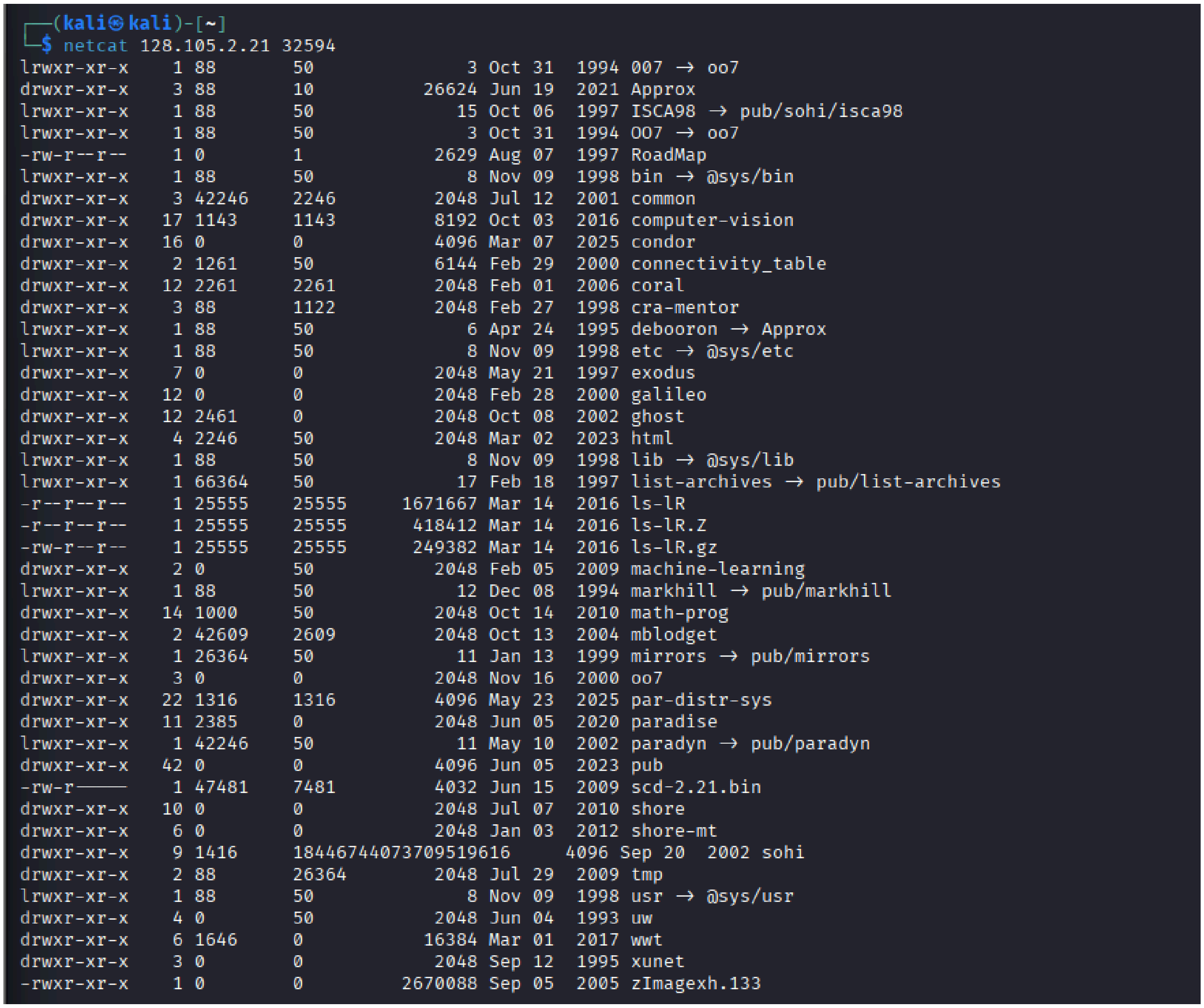


```
MATCH * soundex orange
152 166 matches found
gcide "Oaring"
gcide "Orang"
gcide "orang"
gcide "Orange"
gcide "orange"
gcide "Orange bird"
gcide "Orange cowry"
```

Exercise 2

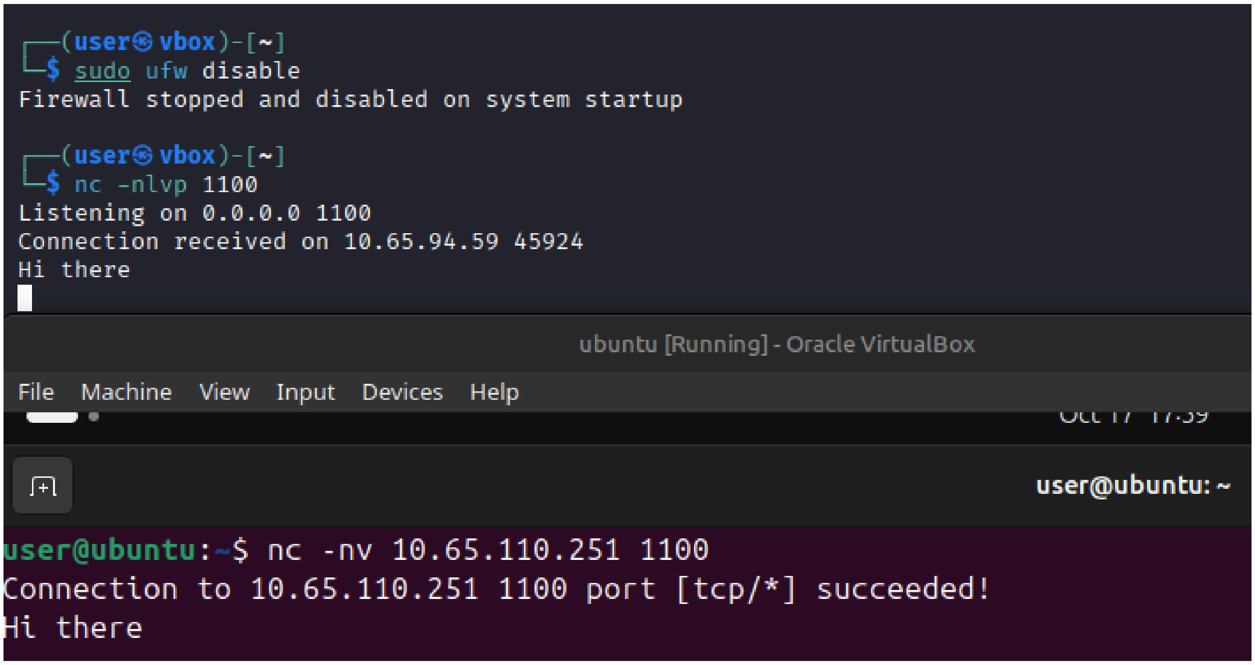
1. 

```
┌──(kali㉿kali)-[~]
└─$ netcat ftp.cs.wisc.edu 21
220 (vsFTPd 3.0.5)
USER anonymous
331 Please specify the password.
PASS anonymous
230 Login successful.
PDW
500 Unknown command.
PASV
227 Entering Passive Mode (128,105,2,21,246,181).
PWD
257 "/" is the current directory
PASV
227 Entering Passive Mode (128,105,2,21,127,82).
lsit
500 Unknown command.
list
150 Here comes the directory listing.
226 Directory send OK.
quit
221 Goodbye.
```



```
┌──(kali㉿kali)-[~]
└─$ netcat 128.105.2.21 32594
lrwxr-xr-x    1 88        50                3 Oct 31  1994 007 → oo7
drwxr-xr-x    3 88        10            26624 Jun 19  2021 Approx
lrwxr-xr-x    1 88        50               15 Oct 06  1997 ISCA98 → pub/sohi/isca98
lrwxr-xr-x    1 88        50                3 Oct 31  1994 OO7 → oo7
-rw-r--r--    1 0         1              2629 Aug 07  1997 RoadMap
lrwxr-xr-x    1 88        50                8 Nov 09  1998 bin → @sys/bin
drwxr-xr-x    3 42246     2246           2048 Jul 12  2001 common
drwxr-xr-x   17 1143      1143           8192 Oct 03  2016 computer-vision
drwxr-xr-x   16 0         0              4096 Mar 07  2025 condor
drwxr-xr-x    2 1261      50             6144 Feb 29  2000 connectivity_table
drwxr-xr-x   12 2261      2261           2048 Feb 01  2006 coral
drwxr-xr-x    3 88        1122           2048 Feb 27  1998 cra-mentor
lrwxr-xr-x    1 88        50                6 Apr 24  1995 debooron → Approx
lrwxr-xr-x    1 88        50                8 Nov 09  1998 etc → @sys/etc
drwxr-xr-x    7 0         0              2048 May 21  1997 exodus
drwxr-xr-x   12 0         0              2048 Feb 28  2000 galileo
drwxr-xr-x   12 2461      0              2048 Oct 08  2002 ghost
drwxr-xr-x    4 2246      50             2048 Mar 02  2023 html
lrwxr-xr-x    1 88        50                8 Nov 09  1998 lib → @sys/lib
lrwxr-xr-x    1 66364     50               17 Feb 18  1997 list-archives → pub/list-archives
-r--r--r--    1 25555     25555       1671667 Mar 14  2016 ls-lR
-r--r--r--    1 25555     25555        418412 Mar 14  2016 ls-lR.Z
-rw-r--r--    1 25555     25555        249382 Mar 14  2016 ls-lR.gz
drwxr-xr-x    2 0         50             2048 Feb 05  2009 machine-learning
lrwxr-xr-x    1 88        50               12 Dec 08  1994 markhill → pub/markhill
drwxr-xr-x   14 1000      50             2048 Oct 14  2010 math-prog
drwxr-xr-x    2 42609     2609           2048 Oct 13  2004 mblodget
lrwxr-xr-x    1 26364     50               11 Jan 13  1999 mirrors → pub/mirrors
drwxr-xr-x    3 0         0              2048 Nov 16  2000 oo7
drwxr-xr-x   22 1316      1316           4096 May 23  2025 par-distr-sys
drwxr-xr-x   11 2385      0              2048 Jun 05  2020 paradise
lrwxr-xr-x    1 42246     50               11 May 10  2002 paradyn → pub/paradyn
drwxr-xr-x   42 0         0              4096 Jun 05  2023 pub
-rw-r-----    1 47481     7481           4032 Jun 15  2009 scd-2.21.bin
drwxr-xr-x   10 0         0              2048 Jul 07  2010 shore
drwxr-xr-x    6 0         0              2048 Jan 03  2012 shore-mt
drwxr-xr-x    9 1416      18446744073709519616     4096 Sep 20  2002 sohi
drwxr-xr-x    2 88        26364          2048 Jul 29  2009 tmp
lrwxr-xr-x    1 88        50                8 Nov 09  1998 usr → @sys/usr
drwxr-xr-x    4 0         50             2048 Jun 04  1993 uw
drwxr-xr-x    6 1646      0             16384 Mar 01  2017 wwt
drwxr-xr-x    3 0         0              2048 Sep 12  1995 xunet
-rwxr-xr-x    1 0         0           2670088 Sep 05  2005 zImagexh.133
```

Exercise 3



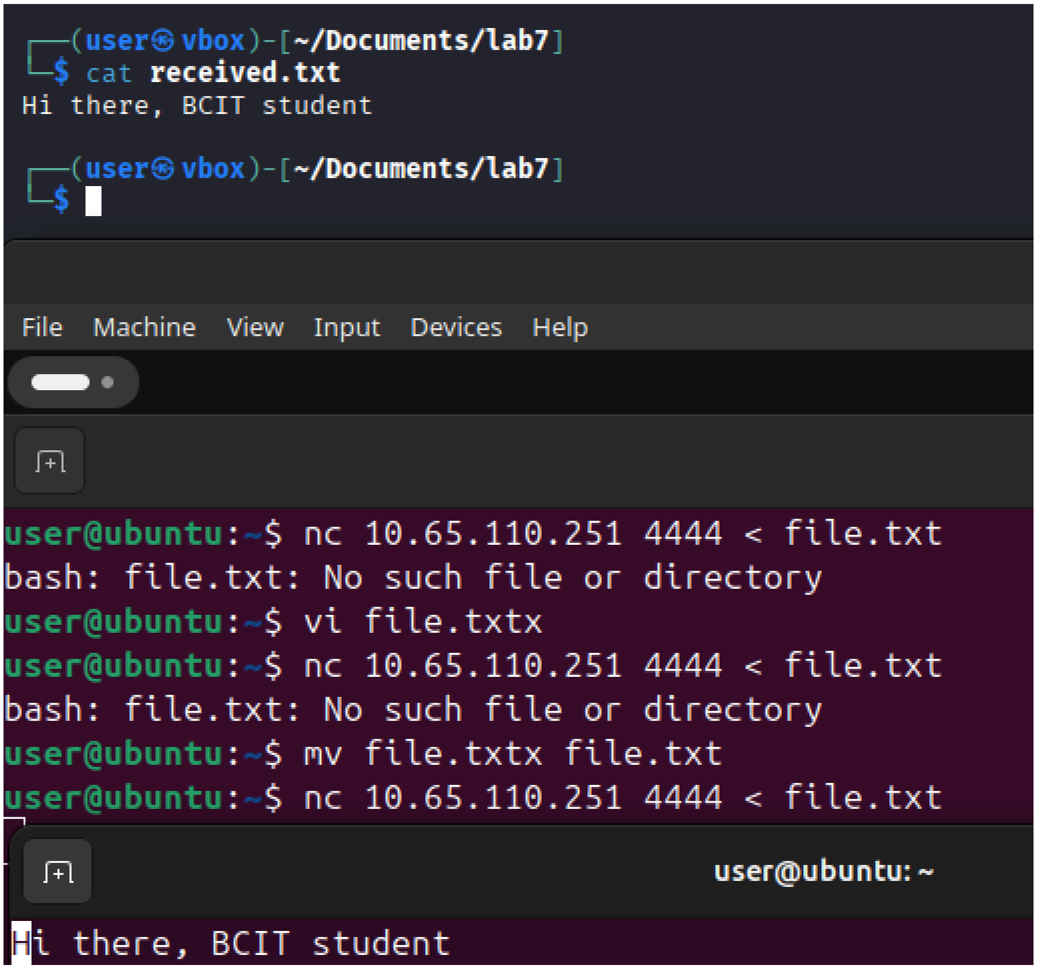
```
┌──(user㉿vbox)-[~]
└─$ sudo ufw disable
Firewall stopped and disabled on system startup

┌──(user㉿vbox)-[~]
└─$ nc -nlvp 1100
Listening on 0.0.0.0 1100
Connection received on 10.65.94.59 45924
Hi there
```

```
user@ubuntu:~$ nc -nv 10.65.110.251 1100
Connection to 10.65.110.251 1100 port [tcp/*] succeeded!
Hi there
```

1. The connection to the server is closed, no further messages can be send
2. No, netcat connect and establishes connection with the first client that connects to the server, if a second clients tries to connect to the server while the first client is still connected, the TCP SYN queue is never complete so it can never connect until first client is disconnected from the server
3. TCP is connection-oriented, meaning that sender and receiver firstly need to establish a connection based on agreed parameters. They do this through as 3-way handshake procedure. The server must be listening for connection requests from clients before a connection is established.

Exercise 4

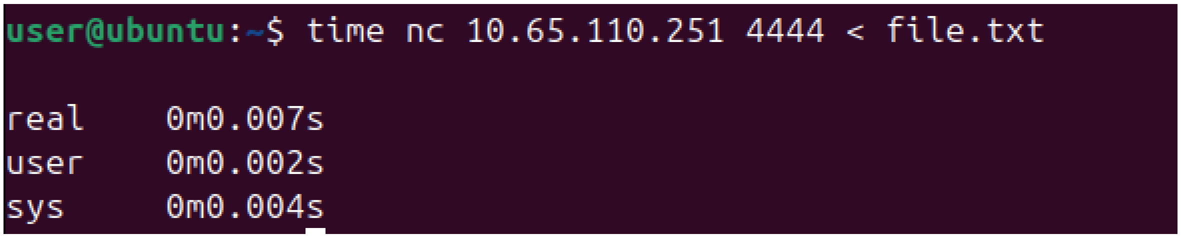


```
┌──(user㉿vbox)-[~/Documents/lab7]
└─$ cat received.txt
Hi there, BCIT student

┌──(user㉿vbox)-[~/Documents/lab7]
└─$ 
```

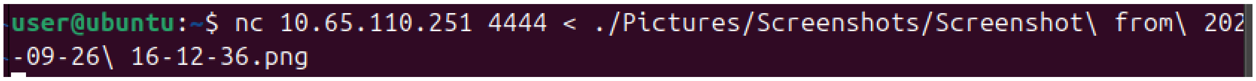
```
user@ubuntu:~$ nc 10.65.110.251 4444 < file.txt
bash: file.txt: No such file or directory
user@ubuntu:~$ vi file.txtx
user@ubuntu:~$ nc 10.65.110.251 4444 < file.txt
bash: file.txt: No such file or directory
user@ubuntu:~$ mv file.txtx file.txt
user@ubuntu:~$ nc 10.65.110.251 4444 < file.txt
```

```
Hi there, BCIT student
```

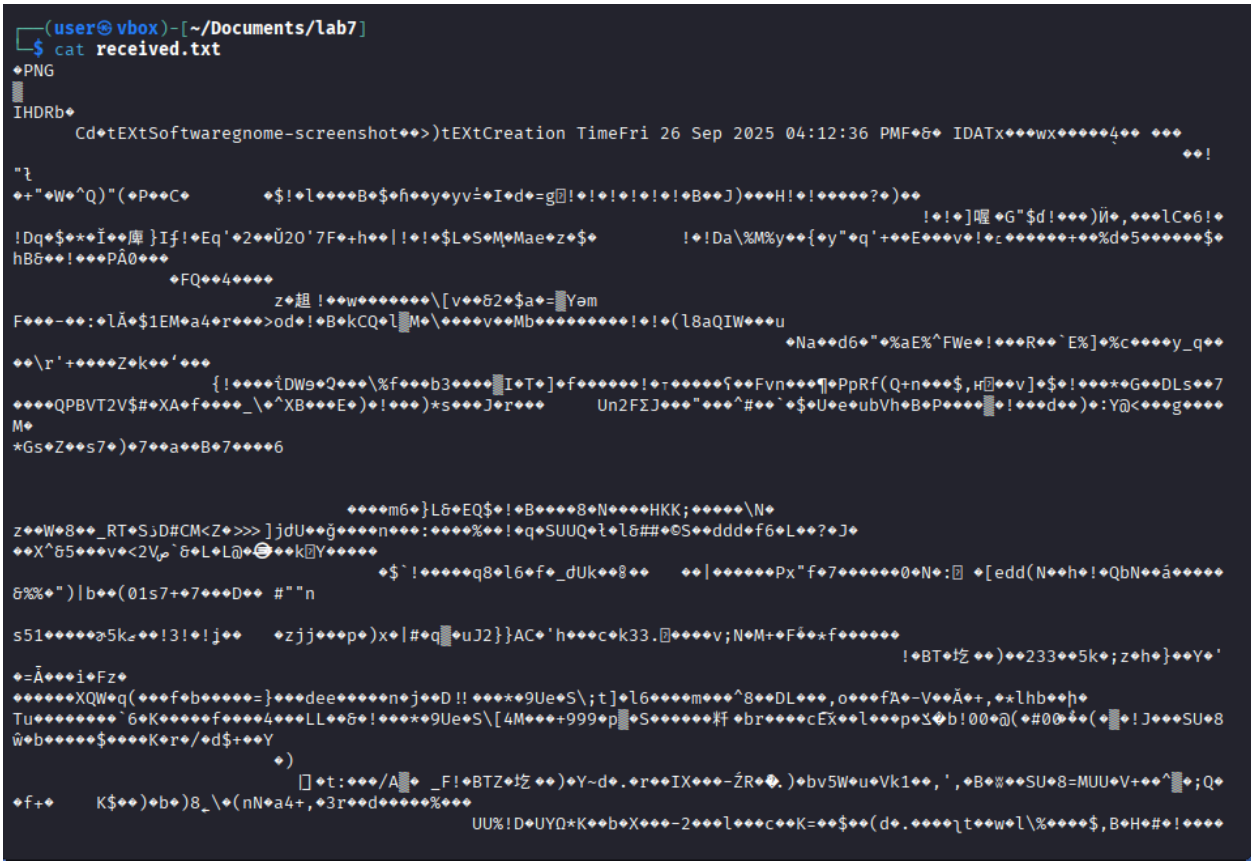


```
user@ubuntu:~$ time nc 10.65.110.251 4444 < file.txt

real	0m0.007s
user	0m0.002s
sys	0m0.004s
```



```
user@ubuntu:~$ nc 10.65.110.251 4444 < ./Pictures/Screenshots/Screenshot\ from\ 202
-09-26\ 16-12-36.png
```



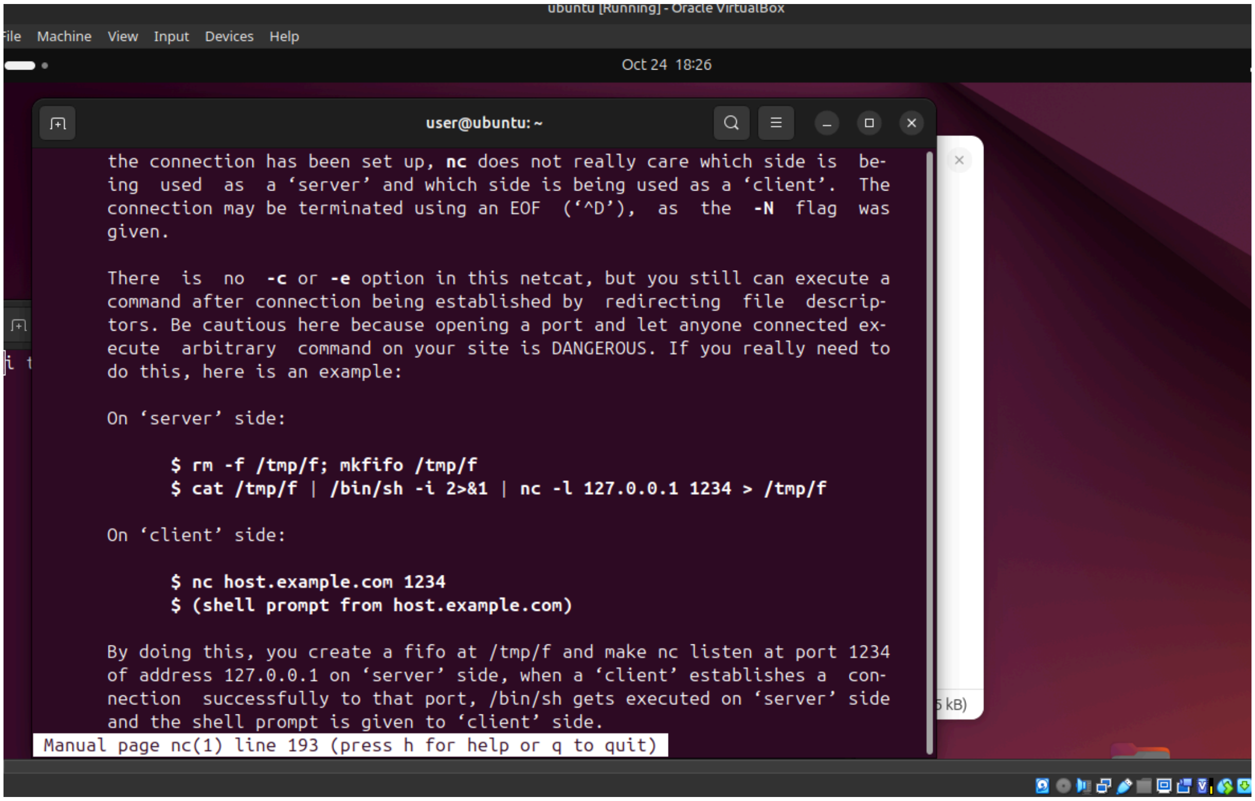
```
┌──(user㉿vbox)-[~/Documents/lab7]
└─$ cat received.txt
�PNG
▒
IHDRb�
      Cd�tEXtSoftwaregnome-screenshot��>)tEXtCreation TimeFri 26 Sep 2025 04:12:36 PMF�&� IDATx���wx�����4�� ���
                                                                                                          ��!
"ɫ
�+"�W�^Q)"(�P��C�       �$!�l����B�$�ħ��y�yv≐�I�d�=g⍰!�!�!�!�!�!�B��J)���H!�!�����?�)��
                                                                                    !�!�]喔�G"$d!���)Й�,���lC�6!�
!Dq�$�*�Ĭ��庫}Iʄ!�Eq'�2��Ŭ2O'7F�+h��|!�!�$L�S�M̦�Mae�z�$�        !�!Da\%M%y��{�y"�q'+��E���v�!�ꞇ������+��%d�5������$�
hB&��!���PÂ0���
            �FQ��4����
                     z�超!��w�������\[v��&2�$a�=▒Yəm
F���-��:�lĂ�$1EM�a4�r���>od�!�B�kCQ�l▒M�\����v��Mb���������!�!�(l8aQIW���u
                                                              �Na��d6�"�%aE%^FWe�!���R��`E%]�%c����y_q��
��\r'+����Z�k��ʻ���
                 {!����îDW૭�Ջ���\%f���b3����▒I�T�]�f������!�ᴛ�����ʕ��Fvn���¶�PpRf(Q+n���$,н⍰��v]�$�!���*�G��DLs��7
����QPBVT2V$#�XA�f����_\�^XB���E�)�!���)*s���J�r���     Un2FΣJ���"���^#��`�$�U�e�ubVh�B�P����▒�!���d��)�:Y@<���g����
M�
*Gs�Z��s7�)�7��a��B�7����6


                          ����m6�}L&�EQ$�!�B����8�N����HKK;�����\N�
z��W�8��_RT�SʖD#CM<Z�>>>]jđU��ğ����n���:����%��!�q�SUUQ�ɫ�l&##�©S��ddd�f6�L��?�J�
��X^&5���v�<2Vص`&�L�L@�㊂��k⍰Y�����
                                  �$`!�����q8�l6�f�_đUk��8��   ��|������Px"f�7������0�N�:⍰ �[edd(N��h�!�QbN��á�����
&%%�")|b��(01s7+�7���D�� #""n

s51�����ङ5kܭ��!3!�!ʝ��   �zjj���p�)x�|#�q▒�uJ2}}AC�'h���c�k33.⍰����v;N�M+�F̈́��*f������
                                                                                  !�BT�圪��)��233��5k�;z�h�}��Y�'
�=Ā���i�Fz�
������XQW�q(���f�b�����=}���dee�����n�j��D‼���*�9Ue�S\;t]�l6����m���^8��DL���,o���fȀ�-V��Ă�+,�*lhb��ɦ�
Tu���������`6�K�����f����4���LL��&�!���*�9Ue�S\[4M���+999�p▒�S������粁�br����cE͂x��l���p�ኋ�b!00�@(�#00ۇ�(�▒�!J���SU�8
ŵ�b�����$����K�r�/�d$+��Y
                         �)
                           ⎕�t:���/A▒� _F!�BTZ�圪��)�Y~d�.�r��IX���-ŹR��.)�bv5W�u�Vk1��,',�B�ꞩ��SU�8=MUU�V+��^▒�;Q�
�f+�    K$��)�b�)8˛\�(nN�a4+,�3r��d�����%���
                                             UU%!D�UYΩ*K��b�X���-2���l���c��K=��$��(d�.����ʅt��w�l\%����$,B�H�#�!����
```

TCP transmits raw bytes not texts so it will transfer the PNG successfully

Exercise 5



ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Oct 24 18:26
user@ubuntu: ~

```
       the connection has been set up, nc does not really care which side is  be‐
       ing  used  as  a ‘server’ and which side is being used as a ‘client’.  The
       connection may be terminated using an EOF  (‘^D’),  as  the  -N  flag  was
       given.

       There  is  no  -c or -e option in this netcat, but you still can execute a
       command after connection being established by  redirecting  file  descrip‐
       tors. Be cautious here because opening a port and let anyone connected ex‐
       ecute  arbitrary  command on your site is DANGEROUS. If you really need to
       do this, here is an example:

       On ‘server’ side:

             $ rm -f /tmp/f; mkfifo /tmp/f
             $ cat /tmp/f | /bin/sh -i 2>&1 | nc -l 127.0.0.1 1234 > /tmp/f

       On ‘client’ side:

             $ nc host.example.com 1234
             $ (shell prompt from host.example.com)

       By doing this, you create a fifo at /tmp/f and make nc listen at port 1234
       of address 127.0.0.1 on ‘server’ side, when a ‘client’ establishes a  con‐
       nection  successfully to that port, /bin/sh gets executed on ‘server’ side
       and the shell prompt is given to ‘client’ side.
 Manual page nc(1) line 193 (press h for help or q to quit)
```

There is no -e option to remotely execute commands on victim’s machine, alternatively can use ssh for a trusted secure connection.

1. Unathorized access, privilege escalation, full compromise of the machines, dara extraction
2. Enable ufw firewall, only allowing or open necessary ports, Setup logging tools or network traffic inspection tools.
3. SSH is safeer because it provide authentication, encryption, auditing and control