

Using Netcat to Understand FTP

BUPT/QMUL

5/3/2017



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

Electronic Engineering 

Mission

- Use nc (netcat) to connect FTP server
 - Learn about passive mode and active mode of FTP
 - Learn about control connection and data connection of FTP
 - Open control connection and data connection in **Passive & Active mode**
 - Compare FTP command and User command
- Use Wireshark to get familiar with FTP
 - Learn about the FTP protocol field
 - Learn about commands and replies of FTP

Steps of passive mode

1. FTP server : 10.3.255.85 gjxy2017/student
2. Open xShell or Terminal, use nc to establish “control connection” to the FTP server: *nc 10.3.255.85 21*
3. login with USER and PASS commands.
4. Input command “PASV” and calculate port number for “data connection” port: *port number = p1 × 256 + p2*, where p1 and p2 are taken from the server’s response.
5. Open another xShell or terminal, then set up “data connection” with calculated number: *nc 10.3.255.85 <port>*
6. Switch to “control connection” and input command “LIST”. Then switch to “data connection” to see the result.
7. Repeat 4~6 with other control command.



Please replace <port> with the calculated port number!!!

Example of FTP passive mode

- In xShell 1, use **nc** to connect with port 21 (control connection port).
- Then use USER and PASS to login FTP.

```
student@BUPTIA:~$ nc 10.3.255.85 21
220-FileZilla Server 0.9.56 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
USER gjxy2017
331 Password required for gjxy2017
PASS student
230 Logged on
```

- Input PASV to enter **passive mode** and get the port number

```
PASV
227 Entering Passive Mode (10,3,255,85,108,222)
```

- Passive port should be: $108 \times 256 + 222 = \underline{27870}$

Example of FTP passive mode

- Switch to xShell 2. Use nc to connect with port 27870 (data connection port) that calculated previously.
- No data will be transfer at first.

```
student@BUPTIA:~$ nc -v 10.3.255.85 27870
Connection to 10.3.255.85 27870 port [tcp/*] succeeded!
```

No data at first

- Switch to xShell 1 and input *LIST*

```
LIST
150 Opening data channel for directory listing of "/"
226 Successfully transferred "/"
```

Example of FTP passive mode

- Switch to xShell 2. Then you get the list of files on FTP server.

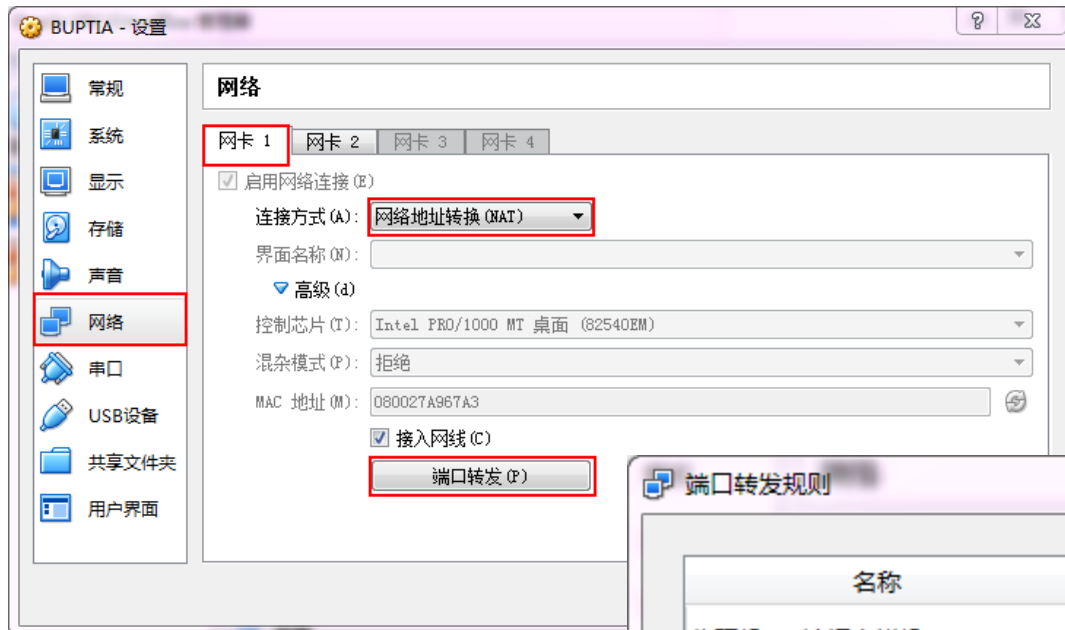
```
student@BUPTIA:~$ nc -v 10.3.255.85 27870
Connection to 10.3.255.85 27870 port [tcp/*] succeeded!

-r--r--r-- 1 ftp ftp      328353 Feb 26  2017 0-Outline-20170227.pdf
-r--r--r-- 1 ftp ftp     1043725 Feb 26  2017 1-Introduction-20170227.pdf
-r--r--r-- 1 ftp ftp     1064489 Mar 06  2017 2-Network Definition .pdf
-r--r--r-- 1 ftp ftp      295517 Mar 13  2017 3-Network Programming-20170313.pdf
-r--r--r-- 1 ftp ftp      714055 Mar 22  2017 4-NetworkProgramming-20170322.pdf
-r--r--r-- 1 ftp ftp      989451 Mar 28  2017 5-NetworkProgramming-20170328.pdf
-r--r--r-- 1 ftp ftp     1997340 Apr 06  2017 6-DHCP-20170401.pdf
-r--r--r-- 1 ftp ftp     1449354 Apr 18  2017 7-DNS-20170410.pdf
-r--r--r-- 1 ftp ftp     1595330 Apr 18  2017 8-TELNET-20170417.pdf
-r--r--r-- 1 ftp ftp     1264023 May 02  2017 9-FTP-20170424.pdf
drwxr-xr-x 1 ftp ftp          0 Apr 25  2017 DHCP&DNS_report
drwxr-xr-x 1 ftp ftp          0 Feb 27  2017 LabSoftware

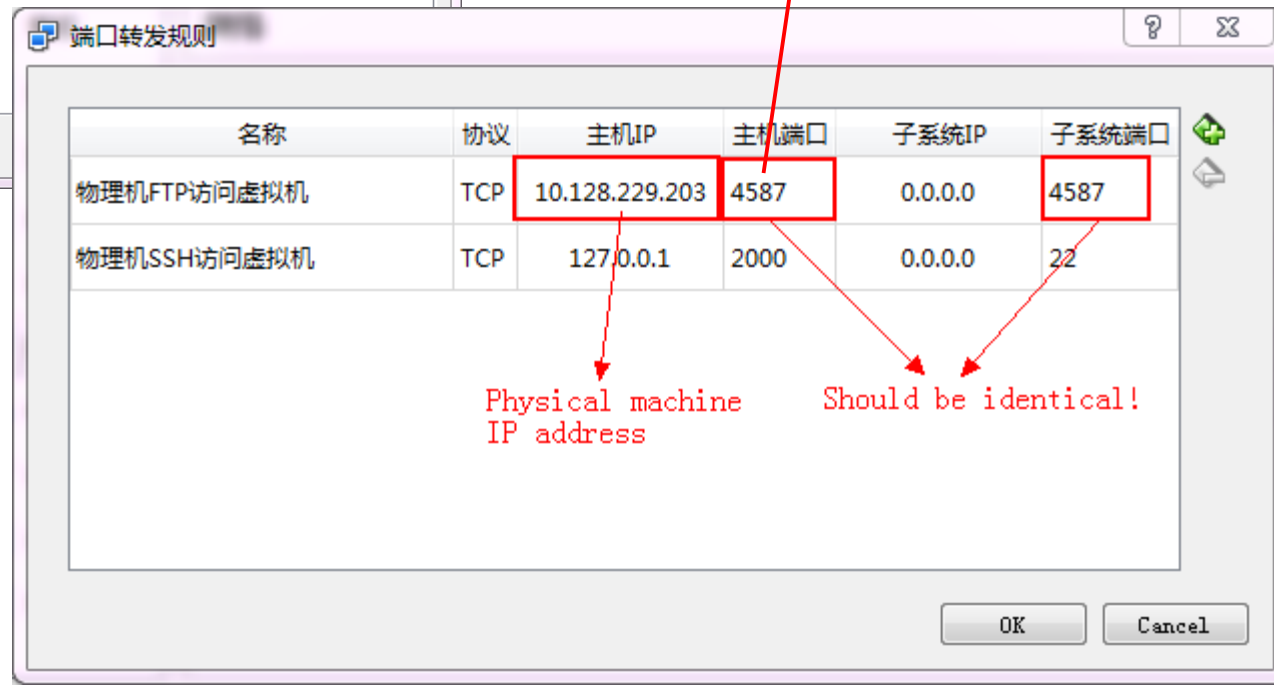
student@BUPTIA:~$
```

Data

Prepare for FTP active mode



Any number smaller than 65535
and bigger than 1024



Example of FTP active mode

- In xShell 1, use **nc** to connect with port 21 (control connection port).
- Then use USER and PASS to login FTP.

```
student@BUPTIA:~$ nc 10.3.255.85 21
220-FileZilla Server 0.9.56 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
USER gjxy2017
331 Password required for gjxy2017
PASS student
230 Logged on
```

- Input **PORT 10,128,229,203,17,235** to enter active mode

```
PORT 10,128,229,203,17,235
200 Port command successful
```



Your physical machine
IP address

$4587 / 256 = 17$

$4587 \bmod 256 = 235$

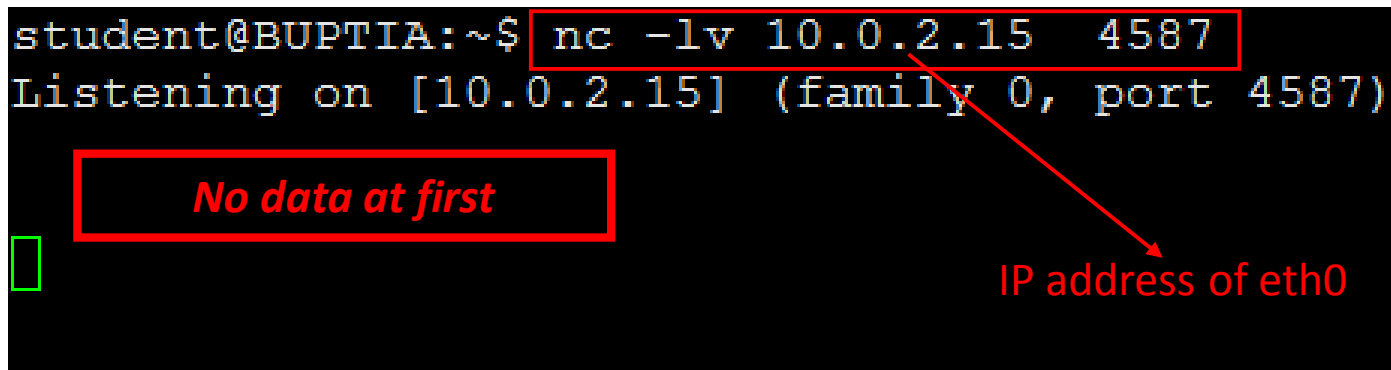
Example of FTP active mode

- Switch to xShell 2. Use nc to listen to ip address of eth0 and port 4587 (data connection port) that selected previously.
- No data will be transfer at first.

```
student@BUPTIA:~$ nc -lv 10.0.2.15 4587
Listening on [10.0.2.15] (family 0, port 4587)
```

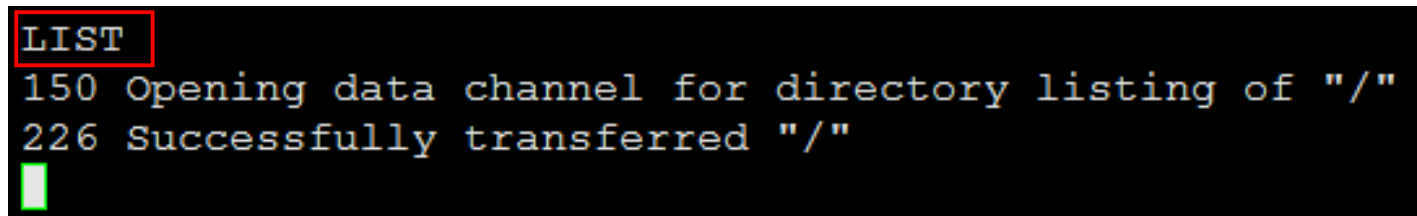
No data at first

IP address of eth0



- Switch to xShell 1 and input **LIST**

```
LIST
150 Opening data channel for directory listing of "/"
226 Successfully transferred "/"
```



Example of FTP active mode

```
student@BUPTIA:~$ nc -lv 10.0.2.15 4587
Listening on [10.0.2.15] (family 0, port 4587)

Connection from [10.0.2.2] port 4587 [tcp/*] accepted (family 2, sport
-r--r--r-- 1 ftp ftp          328353 Feb 26 2017 0-Outline-20170227.pdf
-r--r--r-- 1 ftp ftp          1043725 Feb 26 2017 1-Introduction-201702
-r--r--r-- 1 ftp ftp          1064489 Mar 06 2017 2-Network Definition
-r--r--r-- 1 ftp ftp           295517 Mar 13 2017 3-Network Programming
-r--r--r-- 1 ftp ftp           714055 Mar 22 2017 4-NetworkProgramming-
-r--r--r-- 1 ftp ftp           989451 Mar 28 2017 5-NetworkProgramming-
-r--r--r-- 1 ftp ftp          1997340 Apr 06 13:10 6-DHCP-20170401.pdf
-r--r--r-- 1 ftp ftp          1449354 Apr 18 14:21 7-DNS-20170410.pdf
-r--r--r-- 1 ftp ftp          1595330 Apr 18 14:21 8-TELNET-20170417.pdf
-r--r--r-- 1 ftp ftp          1264023 May 02 09:01 9-FTP-20170424.pdf
drwxr-xr-x 1 ftp ftp           0 Apr 25 16:31 DHCP&DNS_report
drwxr-xr-x 1 ftp ftp           0 Feb 27 2017 LabSoftware
student@BUPTIA:~$
```

Data

Try ...

- USER, PASS, PASV, PWD, CWD, CDUP, LIST, QUIT ... (as passible as your can)
- You can also input command “HELP” in *control connection* to find all FTP command.

```
PASV
227 Entering Passive Mode (10,128,229,203,17,235)
LIST
150 Connection accepted
226 Transfer OK
HELP
214-The following commands are recognized:
  USER  PASS  QUIT  CWD  PWD  PORT  PASV  TYPE
  LIST  REST  CDUP  RETR  STOR  SIZE  DELE  RMD
  MKD   RNFR  RNT0  ABOR  SYST  NOOP  APPE  NLST
  MDTM  XPWD  XCUP  XMKD  XRMD  NOP   EPSV  EPRT
  AUTH  ADAT  PBSZ  PROT  FEAT  MODE  OPTS  HELP
  ALLO  MLST  MLSD  SITE  P@SW  STRU  CLNT  MFMT
  HASH
214 Have a nice day.
█
```

Use Wireshark to get familiar with FTP

- For wireshark usage, refer to Lab08-DHCPDNS.pdf
 - Capture on interface eth0 of ubuntu
- Display filter
 - Control connection: **ftp** or **tcp.port==21**
 - Data connection
 - ✓ Active mode: **ftp-data** or **tcp.port==20**
 - ✓ Passive mode: **tcp.port==<calculated port number>**
- Analyze protocol field of FTP packets
- Find commands and replies in FTP packets