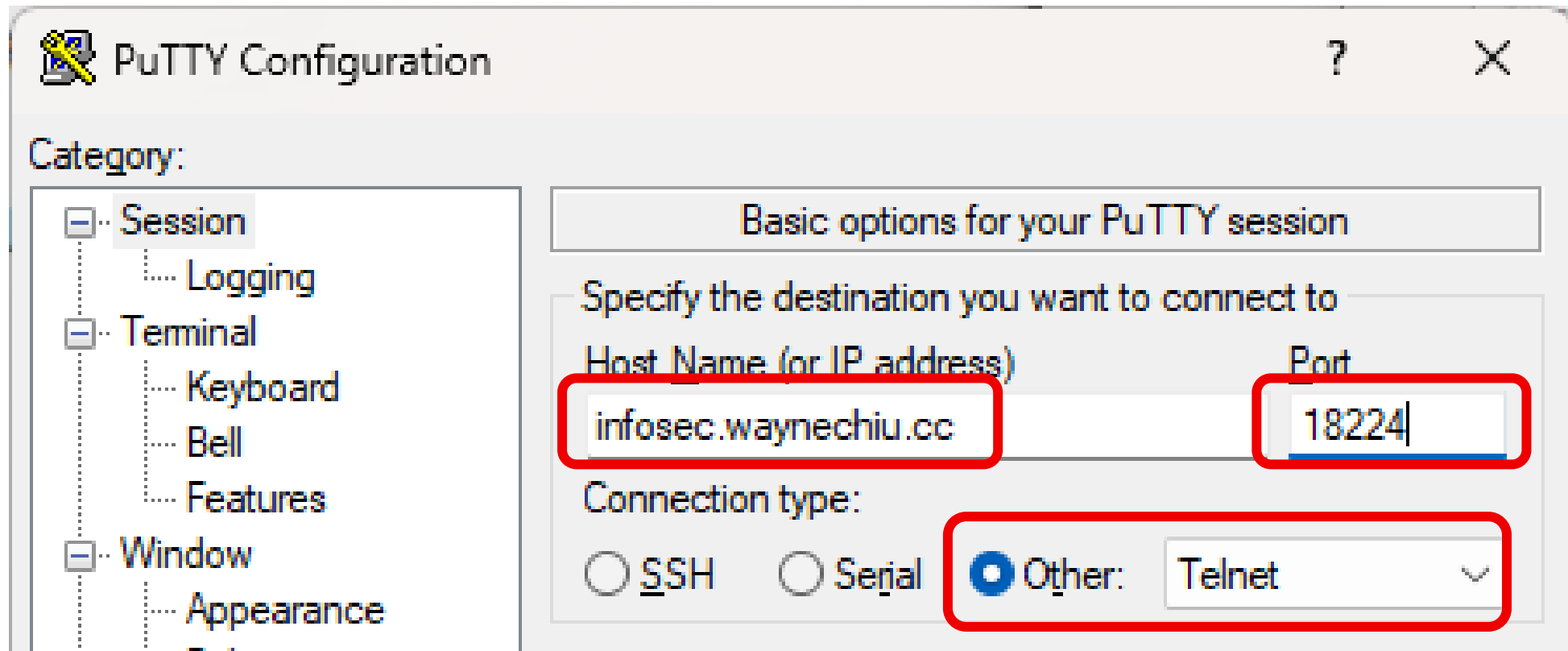


Lancaster University

Network Security Lab 06 Instruction

1. Have your telnet client ready



2. Connect to the server.

It might take a while sometimes.

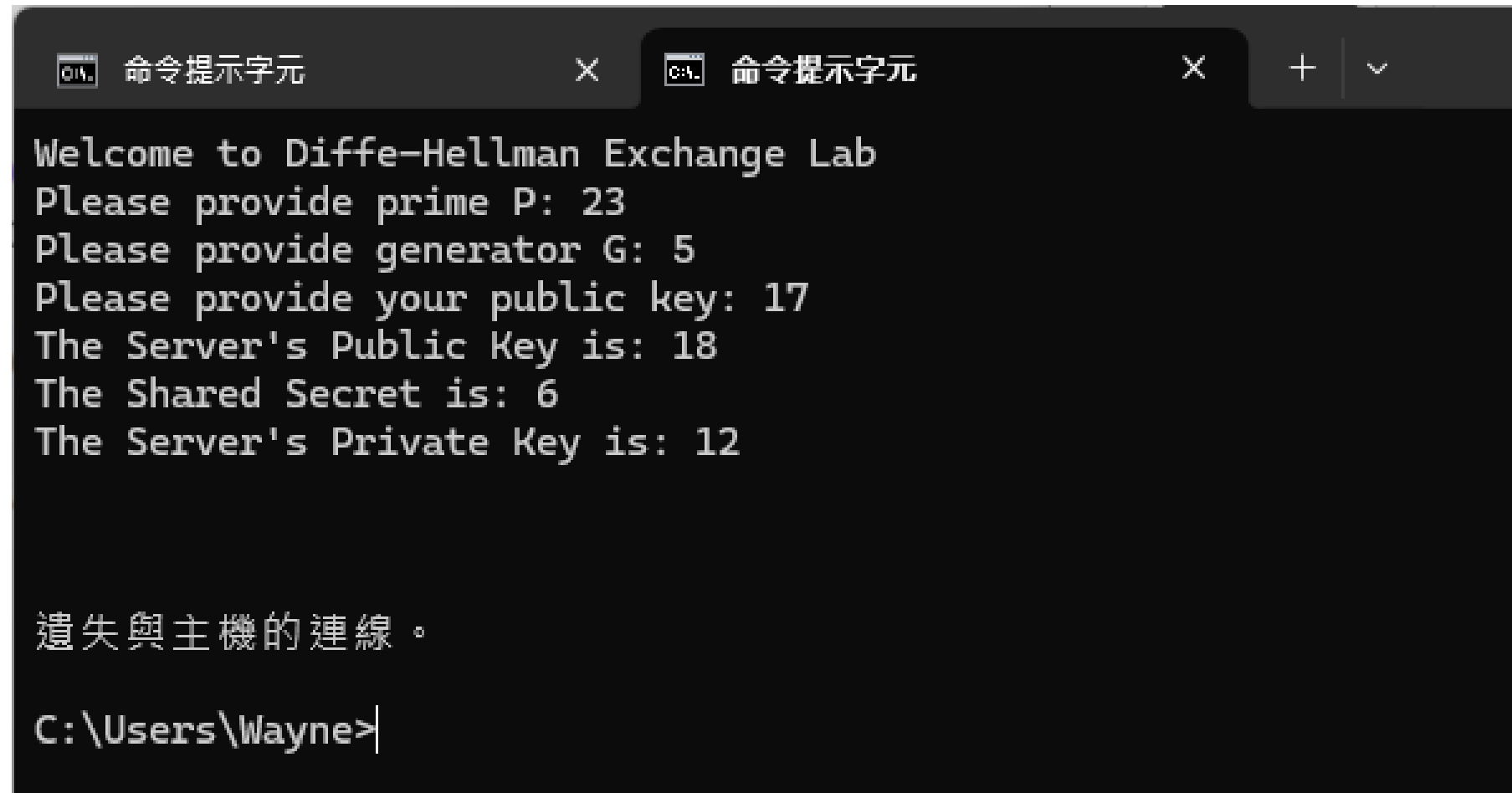
infosec.waynechiu.cc - PuTTY

```
Welcome to Diffie-Hellman Exchange Lab  
Please provide prime P: █
```

3. Provide sufficient information

- 1. Determine A Prime (P) and Modular Root of Prime (G)
- 2. Determine your secret, calculate, and provide your public key
- 3. The Server will then provide its public key.
- 4. Try to perform your calculation to check whether both of you have the same shared secret.

4. Example



```
命令提示字元
Welcome to Diffie-Hellman Exchange Lab
Please provide prime P: 23
Please provide generator G: 5
Please provide your public key: 17
The Server's Public Key is: 18
The Shared Secret is: 6
The Server's Private Key is: 12

遺失與主機的連線。

C:\Users\Wayne>
```

5. –Nix (Linux and Unix-like)

- Usually, the **tool telnet is usually built-in** within the operating system:
 - Open your terminal program
 - Command: `telnet <ip> <port>`
 - Example:

A screenshot of a terminal window with a dark background. The title bar at the top shows a window icon and the text 'wayne@FDL-Wayne-DELL:~'. The terminal content shows the prompt 'wayne@FDL-Wayne-DELL:~\$' followed by the command 'telnet 213.136.8.188 23'. A white cursor is positioned at the end of the command.

```
wayne@FDL-Wayne-DELL:~$ telnet 213.136.8.188 23
```

5. If your –Nix system does not have telnet.

1

[Packet Safari - Wireshark-In-A-Page](#)

[PuTTY - A SSH/TELNET Client For Windows](#)

If you are running -nix system, install TELNET.

[telnet_client - A Standalone Simple TELNET Client for Linux/Unix](#)

[I need instructions.](#)

Right click and save the file.

2

```
wayne@FDL-Wayne-DELL:~/下载
~/下载
wayne@FDL-Wayne-DELL:~/下载$ gcc -o ./telnet_client ./telnet_client.c
wayne@FDL-Wayne-DELL:~/下载$
```

`gcc -o ./telnet_client ./telnet_client.c`

Compile the source code within the directory

3

```
wayne@FDL-Wayne-DELL:~/下载
~/下载
wayne@FDL-Wayne-DELL:~/下载$ ./telnet_client
Usage: ./telnet_client [IPv4-address] [port]
wayne@FDL-Wayne-DELL:~/下载$ ./telnet_client 213.136.8.188 23
```

`./telnet_client [ipv4] [port]`

Connect the server with compiled program