

【2021 Advanced Computer Networks Homework 5】

【簡介】

使用 c 語言製作 subnet IP scanner，

首先取得輸入 interface 的 ip 和 netmask，

之後依序對同個網段的主機發出 ICMP request，確認對方是否存在

【指令】

編譯

```
make
```

執行

```
sudo ./ipscanner -i INTERFACE -t TIMEOUT
```

【執行結果】

1. ifconfig

The image shows a terminal window with a dark purple background. The title bar at the top indicates the system is running Ubuntu 22.04 LTS, with the date and time '12月 22 15:10' and the user 'en'. The terminal prompt is 'miksuki@miksuki-BM6AE-BM1AE-BP1AE: ~'. The user has entered several commands to configure network interfaces. The output for the 'eno1' interface shows it is configured with IP 140.117.168.64 and netmask 255.255.255.0. The output for the 'lo' interface shows it is configured with IP 127.0.0.1 and netmask 255.0.0.0. The terminal also shows the status of the interfaces and the amount of data received and transmitted.

```
miksuki@miksuki-BM6AE-BM1AE-BP1AE:~$
miksuki@miksuki-BM6AE-BM1AE-BP1AE:~$
miksuki@miksuki-BM6AE-BM1AE-BP1AE:~$
miksuki@miksuki-BM6AE-BM1AE-BP1AE:~$ ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 140.117.168.64  netmask 255.255.255.0  broadcast 140.117.168.255
    inet6 fe80::d152:b2bd:d428:a095  prefixlen 64  scopeid 0x20<link>
           txqueuelen 1000  (Ethernet)
    RX packets 131151745  bytes 17058610047 (17.0 GB)
    RX errors 0  dropped 2321867  overruns 0  frame 0
    TX packets 5992443  bytes 656095571 (656.0 MB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
    device interrupt 20  memory 0xf7c00000-f7c20000

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 650660  bytes 93163589 (93.1 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 650660  bytes 93163589 (93.1 MB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

miksuki@miksuki-BM6AE-BM1AE-BP1AE:~$
```

2. 輸入錯誤指令

[illegible]

3. 輸入正確指令

The screenshot shows a Visual Studio Code window with a terminal open. The terminal title is "makefile - TCPIP - Visual Studio Code". The terminal content shows a user running a netmask scan using nmap. The output indicates that the IP 140.117.168.64 is open, while the others are unreachable.

```
miksuki@miksuki-BMGAE-BM1AE-BP1AE:~/Desktop/TCPIP/hw5$  
miksuki@miksuki-BMGAE-BM1AE-BP1AE:~/Desktop/TCPIP/hw5$  
miksuki@miksuki-BMGAE-BM1AE-BP1AE:~/Desktop/TCPIP/hw5$  
miksuki@miksuki-BMGAE-BM1AE-BP1AE:~/Desktop/TCPIP/hw5$  
miksuki@miksuki-BMGAE-BM1AE-BP1AE:~/Desktop/TCPIP/hw5$  
miksuki@miksuki-BMGAE-BM1AE-BP1AE:~/Desktop/TCPIP/hw5$  
miksuki@miksuki-BMGAE-BM1AE-BP1AE:~/Desktop/TCPIP/hw5$ sudo ./ipscanner -i enol -t 1  
my ip: 140.117.168.64  
my netmask: 255.255.255.0  
my interface: enol  
my pid: 4114  
TIMEOUT: 100ms  
  
-----  
start scan  
-----  
  
PING 140.117.168.1 (data size = 10, id = 4114, seq = 1, timeout = 100ms)  
Destination unreachable  
PING 140.117.168.2 (data size = 10, id = 4114, seq = 2, timeout = 100ms)  
Destination unreachable  
PING 140.117.168.3 (data size = 10, id = 4114, seq = 3, timeout = 100ms)  
Destination unreachable  
PING 140.117.168.4 (data size = 10, id = 4114, seq = 4, timeout = 100ms)  
Reply from 140.117.168.4 : time = 3.036000ms  
PING 140.117.168.5 (data size = 10, id = 4114, seq = 5, timeout = 100ms)  
Reply from 140.117.168.5 : time = 1.909000ms  
PING 140.117.168.6 (data size = 10, id = 4114, seq = 6, timeout = 100ms)  
Destination unreachable  
PING 140.117.168.7 (data size = 10, id = 4114, seq = 7, timeout = 100ms)  
Destination unreachable  
PING 140.117.168.8 (data size = 10, id = 4114, seq = 8, timeout = 100ms)  
Destination unreachable  
PING 140.117.168.9 (data size = 10, id = 4114, seq = 9, timeout = 100ms)  
Destination unreachable  
PING 140.117.168.10 (data size = 10, id = 4114, seq = 10, timeout = 100ms)  
Destination unreachable
```

4. request packet

The image shows a Wireshark packet capture of an ICMP Echo (ping) request and response. The packet list on the left shows packet 303273 selected. The packet details pane on the right shows the structure of the ICMP Echo request, including the Identifier (64785), Sequence number (5), and Checksum (0xc345). The packet bytes pane shows the raw data in hexadecimal and ASCII, with the response frame starting at offset 0056.