Name ..... ID ..... Section ..... Seat No .....

Sirindhorn International Institute of Technology
Thammasat University

Midterm Exam: Semester 2, 2010

Course Title: ITS332 Information Technology Laboratory II

Instructor: Steven Gordon

Date/Time: Friday 24 December 2010; 13:30–15:00

Instructions:

- This examination paper has 19 pages (including this page).
- Conditions of Examination: Closed book; No dictionary; Non-programmable calculator is allowed
- Students are not allowed to be out of the exam room during examination. Going to the restroom may result in score deduction.
- Students are not allowed to have communication devices (e.g. mobile phone) in their possession.
- Write your name, student ID, section, and seat number clearly on the front page of the exam, and on any separate sheets (if they exist).
- Assume the user in all questions has administrator privileges (that is, you can ignore the need for `sudo`).
- Each question part is worth 1 mark, unless otherwise stated.
- Reference material at the end of the exam may be used.

Question 1 [7 marks]

A command was run on computer A with IP address `12.23.45.67`. The output of the command is below:

```
Address          HWtype  HWaddress           Flags Mask  Iface
12.23.45.211     ether   00:21:45:55:e5:73   C           eth3
12.23.45.10      ether   00:23:69:3a:f4:7d   C           eth3
12.23.45.29      ether   00:17:31:e7:33:21   C           eth3
12.23.45.47      ether   00:17:31:61:c3:c5   C           eth3
12.23.45.104     ether   00:17:31:5a:e5:89   C           eth3
```

(a) What was the command?

(b) What is the name of the protocol that the output shows information for? You may give the full name or abbreviation.

(c) Draw a message sequence diagram that illustrates how the last line in the above table was learnt using the protocol. Make sure the sender/receivers are clearly shown/explained. [2 marks]

Now consider also the output of another command run on computer B with IP address `12.23.45.29`. There is also computer C with IP address `22.33.44.55` and computer D with IP address `12.23.45.47`.

```
Destination  Gateway      Genmask         Flags Metric Ref Use Iface
12.23.45.0   0.0.0.0      255.255.255.0   U     0      0     0 eth3
0.0.0.0      12.23.45.10  0.0.0.0         UG    100    0     0 eth3
```

(d) What was the commad?

(e) If computer B has an IP datagram to send to computer C, what is the destination hardware address in the Ethernet frame sent?

(f) If computer B has an IP datagram to send to computer D, what is the destination hardware address in the Ethernet frame sent?

Question 2 [6 marks]

The following shows portion of an example log from Apache web server running on the computer with domain name `www.example.com`. Assume no firewalls or proxies in the network.

```
61.19.242.176 - - [05/Dec/2010:08:21:52 +0700] "GET /index.html HTTP/1.0"
 200 1200 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB;
rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:21:53 +0700] "GET /css/main.css
HTTP/1.0" 200 540 "http://www.example.com/index.html" "Mozilla/5.0
(Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12) Gecko/20080201
Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:21:59 +0700] "GET /about/contact.html
HTTP/1.0" 200 906 "http://www.example.com/index.html" "Mozilla/5.0
(Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12) Gecko/20080201
Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:22:30 +0700] "GET /exams/midterm.html
HTTP/1.0" 200 906 "http://www.example.com/about/contact.html"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12)
Gecko/20080201 Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:23:05 +0700] "GET /files/answers.txt
HTTP/1.0" 200 1100 "http://sandilands.info/exams/midterm.html"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12)
Gecko/20080201 Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:23:21 +0700] "GET /index.html HTTP/1.0"
304 20 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12)
Gecko/20080201 Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:23:21 +0700] "GET /css/main.css
HTTP/1.0" 304 20 "http://www.example.com/index.html" "Mozilla/5.0
(Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12) Gecko/20080201
Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:23:45 +0700] "GET
/lectures/handouts.html HTTP/1.0" 200 1330
"http://www.example.com/index.html" "Mozilla/5.0 (Windows; U; Windows
NT 5.1; en-GB; rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12"

61.19.242.176 - - [05/Dec/2010:08:23:54 +0700] "GET /lectures/topic2.html
HTTP/1.0" 404 320 "http://www.example.com/lectures/handouts.html"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12)
Gecko/20080201 Firefox/2.0.0.12"
```

```
61.19.242.176 - - [05/Dec/2010:08:24:22 +0700] "GET /lectures/topic1.html
HTTP/1.0" 200 2303 "http://www.example.com/lectures/handouts.html"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.12)
Gecko/20080201 Firefox/2.0.0.12"
```

Answer the following questions based on the above information.

(a) How many bytes in the file `/index.html`?

(b) What protocol version is used by the web browser to retrieve the web pages?

(c) Which file(s) was requested but does not exist on the server?

(d) The user of the web browser that generated these log entries used the "Back" button on their browser. From the log, describe the entry (or entries) that indicates the user most likely used the Back button, and explain why/how it shows this. [1.5 marks]

(e) There are two requests for `/index.html` in the log. Explain the difference between the responses for each of these requests. [1.5 marks]

Question 3 [7 marks]

Assume the current state of the filesystem in your home directory on a Linux computer is:

```
/home/user/
/home/user/file1.txt
/home/user/file2.txt
/home/user/file3.c
/home/user/code/
/home/user/code/client.c
/home/user/code/server.c
/home/user/captures/
/home/user/captures/dns.cap
/home/user/captures/ping.cap
```

For example, in the `/home/user` directory there are three files and two sub-directories.

Answer the following questions based only on the above information. For each question, unless otherwise stated, assume you are in the directory `/home/user`. The dollar sign, $, indicates the prompt.

(a) What is the output after the following command is executed?

```
$ pwd
```

(b) What command was used to produce the following output?

```
total 8
drwxr-xr-x 2 user user 4096 2010-12-16 14:33 captures
drwxr-xr-x 2 user user 4096 2010-12-16 14:33 code
-rw-r--r-- 1 user user   47 2010-12-16 14:32 file1.txt
-rw-r--r-- 1 user user 4096 2010-12-16 14:32 file2.txt
-rw-r--r-- 1 user user 9034 2010-12-16 14:33 file3.c
```

For the following questions, assume the commands below have been executed:

```
$ cat file1.txt
This exam is too easy!
I am going to get an A.
$ cp file1.txt file4.txt
$ mv file2.txt captures/
$ man wc
WC(1)                          User Commands                          WC(1)

NAME
       wc - print newline, word, and byte counts for each file
... (rest of text hidden by Steve)
```

(c) What is the output after the following command is executed?

```
$ ls
```

(d) What is the output after the following command is executed?

```
$ wc file4.txt
```

(e) Fill in the four blank spaces (_____) such that the execution of the commands will produce the output shown. [3 marks]

```
$ cd /home/user/_____________

$ mkdir _____________

$ rm _____________

$ mv _____________

$ ls -l
total 4
-rw-r--r-- 1 user user 9034 2010-12-16 14:33 file3.c
-rw-r--r-- 1 user user 7145 2010-12-16 14:33 server.c
drwxr-xr-x 2 user user 4096 2010-12-16 15:07 steve
```

Question 4 [8 marks]

Assume Apache web server has been correctly configured and is running on a computer with IP address `72.16.4.3` and domain name `www.example.com`. For reference, a portion of the configuration file `/etc/apache2/sites-available/default` is given below.

```
<VirtualHost *:80>
ServerName www.example.com
ServerAdmin webmaster@example.com

DocumentRoot /var/www
<Directory />
Options FollowSymLinks
AllowOverride None
</Directory>
<Directory /var/www/>
Options Indexes FollowSymLinks MultiViews
AllowOverride None
Order allow,deny
allow from all
</Directory>
... (rest of text hidden by Steve)
```

Selected files and directories on this computer are:

```
/home/user/
/home/user/web/
/home/user/web/test.html
/etc/apache2/
/etc/apache2/apache2.conf
/etc/apache2/sites-available/
/etc/apache2/sites-available/default
/etc/apache2/passwords.txt
/var/www/
/var/www/index.html
/var/www/contact.html
/var/www/about.html
/var/www/images/
/var/www/images/photo.jpg
/var/www/myfiles/
/var/www/myfiles/questions.html
/var/www/myfiles/answers.html
```

Answer the following questions based on the above information.

(a) A user of a web browser on computer `12.34.56.78` enters the following address into the browser: `http://www.example.com/index.html`. Draw a message sequence diagram that illustrates the exchange of HTTP messages. You must clearly show

the information included in the request, as well as the status code include in the response. Assume no caching is used. [1 mark]

(b) If the web browser is using port 50123, then complete the fields of the following headers for the first packet in the above exchange of HTTP messages. [1.5 marks]

- IP Source address:
- IP Destination address:
- IP Protocol number:
- TCP Source port:
- TCP Destination port:

(c) Assume the user of the web browser now clicks on a link with the following URL: `http://www.example.com/test.html`. Draw a message sequence diagram. [1.5 marks]

Assume now additional information is added to the Apache configuration file (and once correctly configured, Apache is restarted):

```
<Directory "/var/www/myfiles">
   AuthType Basic
   AuthName "Questions and answers"
   AuthUserFile /etc/apache2/passwords.txt
   Require user steve
</Directory>
```

(d) Explain what the following command does?

```
$ sudo htpasswd /etc/apache2/passwords.txt steve -b mysecret
```

(e) Assume the user of the web browser now enters the following URL into the address bar: `http://www.example.com/myfiles/questions.html`. Draw a message sequence diagram. [2 marks]

(f) In the above message sequence diagram, in which message/packet is the password inside?

Question 5 [7 marks]

Consider the following output.

```
$ cat _________________________
nameserver 208.67.220.220
nameserver 10.10.10.9

$ ____________________________________________________________
Server: 208.67.220.220
Address: 208.67.220.220#53

Non-authoritative answer:
www.sandilands.info canonical name = sandilands.info.
Name: sandilands.info
Address: 125.25.46.35

$ ____________________________________________________________
Server: 204.13.248.76
Address: 204.13.248.76#53

Name: sandilands.info
Address: 125.25.46.35
```

(a) Fill in the blank spaces (i.e. give the files/commands typed that would produce the output). [5 marks]

(b) What is the IP address for the domain name `www.sandilands.info`?

(c) The 2nd command states "Non-authoritative answer", while the 3rd command does not. Explain the difference.

Question 6 [8 marks]

Consider the two packets below, captured and displayed using tcpdump/Wireshark (other captured packets are not shown). The relevant details of each of the packets is shown on the subsequent pages. Answer the following questions based on this information.

```
No. Time      Source    Destination     Protocol Info
48  5.316001  0.0.0.0   255.255.255.255 DHCP     DHCP Request
50  5.318745  10.10.1.1 10.10.1.198     DHCP     DHCP ACK
```

(a) Explain which computer(s) receive packet number 48. (*Don't* just give the destination address above)

(b) Explain which computer(s) receive packet number 50. (*Don't* just give the destination address above)

(c) What is the port number used by a DHCP client?

(d) What is the MAC address of the computer that sent packet number 48?

(e) After the above two packets have been exchanged, what is the IP address of the computer that sent packet number 48?

(f) For how long is the computer allowed to use the IP address in part (e)?

(g) Draw the packet structure for packet number 50, indicating the protocols used and size of each header/data in bytes (Hint: UDP header is 8 Bytes; DHCP is called "Bootstrap" in Wireshark). [2 marks]

```
Frame 48 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: 00:17:31:5a:e5:89, Dst: ff:ff:ff:ff:ff:ff
    Destination: ff:ff:ff:ff:ff:ff
    Source: 00:17:31:5a:e5:89
    Type: IP (0x0800)
Internet Protocol, Src: 0.0.0.0, Dst: 255.255.255.255
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x10
    Total Length: 328
    Identification: 0x0000 (0)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
    Header checksum: 0x3996 [correct]
    Source: 0.0.0.0
    Destination: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source port: 68
    Destination port: 67
    Length: 308
    Checksum: 0x0d4d [correct]
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x1a5bb57c
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: 00:17:31:5a:e5:89
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option: (t=53,l=1) DHCP Message Type = DHCP Request
    Option: (t=54,l=4) DHCP Server Identifier = 10.10.1.1
    Option: (t=50,l=4) Requested IP Address = 10.10.1.198
    Option: (t=12,l=6) Host Name = "ginger"
    Option: (t=55,l=13) Parameter Request List
    End Option
    Padding
```

```
Frame 50 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: 00:50:ba:4c:6b:45, Dst: 00:17:31:5a:e5:89
    Destination: 00:17:31:5a:e5:89
    Source: 00:50:ba:4c:6b:45
    Type: IP (0x0800)
Internet Protocol, Src: 10.10.1.1, Dst: 10.10.1.198
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x10
    Total Length: 328
    Identification: 0x0000 (0)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 16
    Protocol: UDP (0x11)
    Header checksum: 0x92bb [correct]
    Source: 10.10.1.1
    Destination: 10.10.1.198
User Datagram Protocol, Src Port: 67, Dst Port: 68
    Source port: 67
    Destination port: 68
    Length: 308
    Checksum: 0x5d3c [correct]
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x1a5bb57c
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.10.1.198
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: 00:17:31:5a:e5:89
    Client hardware address padding: 00000000000000000000
    Magic cookie: (OK)
    Option: (t=53,l=1) DHCP Message Type = DHCP ACK
    Option: (t=54,l=4) DHCP Server Identifier = 10.10.1.1
    Option: (t=51,l=4) IP Address Lease Time = 3 days
    Option: (t=1,l=4) Subnet Mask = 255.255.255.0
    Option: (t=3,l=4) Router = 10.10.1.1
    Option: (t=6,l=8) Domain Name Server = 10.10.10.5
    Option: (t=44,l=8) NetBIOS over TCP/IP Name Server
    End Option
    Padding
```

Question 7 [3 marks]

Consider the packets below, captured and displayed using tcpdump/Wireshark (other captured packets are not shown). Summary details of the first two packets are also shown below. Answer the following questions based on this information.

```
No. Time       Source      Destination Protocol Info
164 19.865857  10.10.1.22  10.10.10.9  ICMP     Echo (ping) request
165 19.866873  10.10.10.9  10.10.1.22  ICMP     Echo (ping) reply
168 20.366485  10.10.1.22  10.10.10.9  ICMP     Echo (ping) request
169 20.367561  10.10.10.9  10.10.1.22  ICMP     Echo (ping) reply
170 20.867145  10.10.1.22  10.10.10.9  ICMP     Echo (ping) request
171 20.868256  10.10.10.9  10.10.1.22  ICMP     Echo (ping) reply
173 21.367850  10.10.1.22  10.10.10.9  ICMP     Echo (ping) request
174 21.368950  10.10.10.9  10.10.1.22  ICMP     Echo (ping) reply
```

```
Frame 164 (192 bytes on wire, 192 bytes captured)
Ethernet II, Src: 00:17:31:5a:e5:89, Dst: 00:50:ba:4c:6b:45
Internet Protocol, Src: 10.10.1.22, Dst: 10.10.10.9
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0 ()
    Checksum: 0x5670 [correct]
    Identifier: 0x3107
    Sequence number: 1 (0x0001)
    Data (150 bytes)

Frame 165 (192 bytes on wire, 192 bytes captured)
Ethernet II, Src: 00:50:ba:4c:6b:45, Dst: 00:17:31:5a:e5:89
Internet Protocol, Src: 10.10.10.9, Dst: 10.10.1.22
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0 ()
    Checksum: 0x5e70 [correct]
    Identifier: 0x3107
    Sequence number: 1 (0x0001)
    Data (150 bytes)
```

(a) What was the command that produced this set of packets? (Note Ctrl-C was *not* used) [2 marks]

(b) Fill in the blanks for the summary output at the end of the command.

```
4 packets transmitted, 4 received, 0% packet loss, time 1503ms

rtt min/avg/max/mdev = ________/1.075/________/0.035 ms
```

Question 8 [4 marks]

Consider the following output.

```
eth0      Link encap:Ethernet  HWaddr 00:23:69:3A:F4:7D
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::217:31ff:fe5a:e589/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4309758 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5360006 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2088540804 (1.9 GiB)  TX bytes:1468392061 (1.3 GiB)

eth1      Link encap:Ethernet  HWaddr 1C:09:B5:23:F5:04
          inet addr:43.12.65.3  Bcast:43.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::800:27ff:fe00:0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:35501138 errors:0 dropped:314 overruns:0 frame:0
          TX packets:9936181 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2536336083 (2.3 GiB)  TX bytes:3832488791 (3.5 GiB)

eth2      Link encap:Ethernet  HWaddr 00:17:31:5A:E7:E8
          inet addr:204.17.3.199  Bcast:204.17.3.255  Mask:255.255.255.0
          inet6 addr: fe80::217:31ff:fe5a:e7e8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4770786 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5640688 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2870991868 (2.6 GiB)  TX bytes:1625112972 (1.5 GiB)

eth3      Link encap:Ethernet  HWaddr 00:23:69:4D:23:E8
          inet addr:10.10.1.184  Bcast:10.10.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:31152058 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4293932 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3344583050 (3.1 GiB)  TX bytes:2165372707 (2.0 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:699 errors:0 dropped:0 overruns:0 frame:0
          TX packets:699 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:55273 (53.9 KiB)  TX bytes:55273 (53.9 KiB)
```

(a) How many Ethernet LAN cards does the computer have?

(b) What information do you know about the manufacturers of the above Ethernet LAN cards?

(c) With the above settings, you realise that `eth1` and `eth2` are mixed up. Write a command that will replace the IP address of `eth2` with that of `eth1`.

(d) Explain the purpose of the `lo` interface.

Reference Material

Below is the syntax of commonly used commands. The values that the user must choose are given enclosed in < and >. Optional fields are enclosed in [and]. You may use this information in your answers.

```
ifconfig [<interface>] [up | down]
ifconfig <interface> <ipaddress> netmask <subnetmask>
ping [-c <count>] [-s <packetsize>] [-i <interval>] <destination>
tracepath <destination>
nslookup <domain> [<dnsserver>]
route [-n]
arp [-n]
dhclient [<interface>]
apache2ctl [start | stop | restart]
htpasswd <passwordfile> <username> [-b <password>]
```

Commonly used files and directories are listed below. You may use this information in your answers.

```
/etc/hosts
/etc/resolv.conf
/etc/network/interfaces
/etc/services
/var/lib/dhcp3/dhclient.leases
/proc/sys/net/ipv4/ip_forward
/var/www/
/etc/apache2/sites-available/default
```

Port numbers used by common applications include:

20 FTP data transfer

21 FTP connection control

22 SSH, secure remote login

23 TELNET, (unsecure) remote login

25 SMTP, email transfer between servers

53 DNS, domain name lookups

67 DHCP server

80 HTTP, web servers

110 POP3, client access to email

123 NTP, network time

443 HTTPS, web servers with secure access

520 RIP, routing protocol

631 IPP, Internet printing

1503 Windows Live Messenger

1512 WINS, Windows naming service

3306 MySQL database server

3723 Blizzard games

5060 SIP, voice/video signalling

5190 ICQ, instant messaging

8080 HTTP proxy server

Protocol numbers for commonly used transport protocols include:

1 ICMP

2 IGMP

6 TCP

17 UDP

33 DCCP

41 IPv6 encapsulation

47 GRE

89 OSPF

Status codes and their meaning for common HTTP responses include:

100 Continue Client should continue to sent the request

200 Ok Requested content is included in response

301 Moved Permanently This and all future requests should be redirected to the given URL

304 Not Modified Requested content has not been modified since last access

401 Unauthorized Requested content requires authentication that has not been provided or is incorrect

403 Forbidden Request is ok, but not allowed to access the requested content

404 Not Found Requested content could not be found on server

503 Service Unavailable Requested server is currently unavailable