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

Sirindhorn International Institute of Technology
Thammasat University

Final Examination: Semester 2/2007

Course Title : ITS 332 – Information Technology II Lab (Networking)

Instructor : Dr Steven Gordon

Date/Time : Wednesday 12 March 2008, 13:30 – 16:30

Instructions:

- This examination paper has 14 pages (including this page).
- Condition of Examination
  Closed book (No dictionary, no calculator)
- Students are not allowed to be out of the exam room during examination. Going to the restroom may result in score deduction.
- Turn off all communication devices (mobile phone etc.) and leave them under your seat.
- Write your name, student ID, section, and seat number clearly on the answer sheet.
- The space on the back of each page can be used if necessary.

IMPORTANT!

For all multiple choice questions in this exam:

- You must clearly CIRCLE the letter for your answer
- Circle either no answer or one answer (circling two or more answers will be counted as an incorrect answer)
- Marking:
  - Correct answer: 2 marks
  - Incorrect answer: -0.5 mark
  - No answer: 0 marks
- If you circle an answer, and then decide on a different answer, you must clearly indicate the old, unwanted answer is no longer valid (e.g. write a comment next to the answer such as “Unwanted answer”).

General Questions [70 marks]

Question 1 [8 marks]

Assume you have an Apache web server with the standard (default) configuration. The server domain name is: `http://www.example.com/` and the root directory for web files is `/var/www`. You then change the configuration (e.g. the `/etc/apache2/sites-available/default` file) and add the following lines:

```
<Directory "/var/www/private">
      AuthType Basic
      AuthName "Restricted Access to Private Content"
      AuthUserFile /etc/apache2/passwd/passwords
      Require user siit
</Directory>
```

The web server stores the following files:

- `/var/www/index.html`
- `/var/www/test.html`
- `/var/www/steve/index.html`
- `/var/www/steve/test.html`
- `/var/www/private/index.html`
- `/var/www/private/test.html`
- `/etc/apache2/passwd/passwords`
- (as well as all the necessary Apache configuration files)

Answer the following questions based on the above information (assuming no cache's are used).

1.1 If a user using a web browser enters the address `http://www.example.com/index.html`:

a) The user will be prompted for a username/password by their web browser
b) A 404 Not Found will be returned by the server
c) The first HTTP request sent from the browser to server will contain the user's username/password
d) The content of the file `index.html` will be sent from the server to the browser, without the user needing to enter a username/password
e) The server will check the file `/etc/apache2/passwd/passwords` to determine if the browser has sent the correct username/password.
f) None of the above.

1.2 If a user using a web browser enters the address `http://www.example.com/private/index.html`:

a) The user will be prompted for a username/password by their web browser
b) A 404 Not Found will be returned by the server
c) The first HTTP request sent from the browser to server will contain the user's username/password
d) The content of the file `index.html` will be sent from the server to the browser, without the user needing to enter a username/password
e) None of the above.

1.3 What program/command was used to create the passwords file?

a) `apache2ctl start`
b) `apache restart`
c) `passwd`
d) `htpasswd`
e) `apacheconf`
f) None of the above.

1.4 A user of the server computer has read access to all files on that server. If they look in the following file, they will be able to immediately read the password of user `siit`:

a) `/etc/apache2/sites-available/default`
b) `/var/www/private/index.html`
c) `/etc/apache2/passwd/passwords`
d) None of the above.

Question 2 [7 marks]

Match the C Internet socket function to the appropriate description of the function. There is only one correct answer for each function.

1. accept()
2. bind()
3. connect()
4. listen()
5. socket()
6. write()
7. read()

2.1 _____ triggers a TCP SYN segment to be sent

2.2 _____ may trigger a TCP data segment to be sent

2.3 _____ associates an IP address and port number to a socket

2.4 _____ creates an endpoint for communication with another computer

2.5 _____ blocks until a TCP SYN segment is received

2.6 _____ blocks until a TCP data segment is received

2.7 _____ marks a socket as able to accept connections

Question 3 [6 marks]

Answer the questions about the following example code segment for a server program:

```
while (1) {
      newsockfd = accept(sockfd, (struct sockaddr *) &cli_addr, &clilen);
      if (newsockfd < 0) error("ERROR on accept");
      pid = fork();
      if (pid < 0) error("ERROR on fork");
      if (pid == 0)  {
            close(sockfd);
            handlerequest(newsockfd, client_address);
            exit(0);
      }
      else {
            close(newsockfd);
      }
}
```

Assume the process that is initially created when the program is executed is the *parent server process*. Also assume no errors occur.

3.1 The parent server process that executes the program will:

a) Execute the `handlerequest()` function if a connection from a client is accepted
b) Create a new child process when `accept()` function is called.
c) Loop continuously, exiting only when the `handlerequest()` function has completed.
d) Create a new child process for each connection request it accepts.
e) None of the above.

3.2 The `accept()` function:

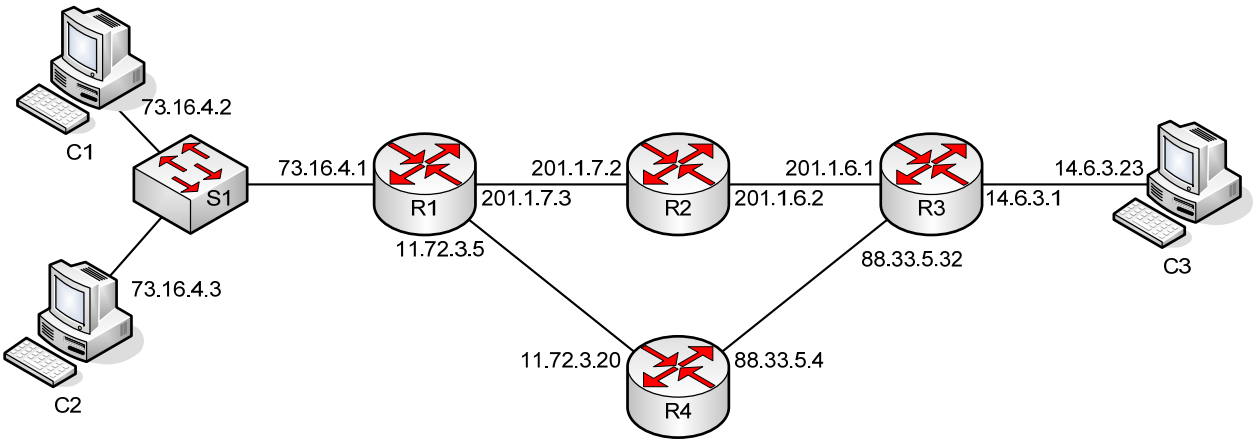
a) Initiates a TCP connection to the client.
b) Is a non-blocking function.
c) Will block until a TCP connection request is received by the client.
d) Will be executed by the child server process, not the parent service process.
e) None of the above.

3.3 If the `handlerequest()` function takes 10 seconds to execute, then:

a) A second client cannot connect to the server within those 10 seconds
b) Clients can only connect to the server at a rate of 1 connection per 10 seconds
c) The rate at which clients can connect to the server is independent of the duration of `handlerequest()`
d) An error will occur if a second client connects to the server within those 10 seconds
e) None of the above.

Question 4 [10 marks]

The figure below illustrates an example IP network. The IP addresses of interfaces are given (the addresses correspond to the nearest interface on the nearest device). Assume all the IP addresses are /24, that is, the first three dotted decimal numbers indicate the network portion of the address, and the last dotted decimal number indicates the host portion of the address.



Answer the following questions based on this network.

4.1 The number of different IP networks used in this example is:

a) 2
b) 3
c) 4
d) 5
e) 6
f) 7

4.2 Complete the routing tables for the four routers. Some entries to the tables are already given; you need to complete the remaining boxes. “Direct” means the router has a direct connection to the destination network. Assume minimum hop routing is used (if there are two paths with the same number of hops, then you may select one). [8 marks]

Router R1

Destination Network	*Next Router*
73.16.4.0	Direct
201.1.7.0	
11.72.3.0	
201.1.6.0	201.1.7.2
88.33.5.0	11.72.3.20
14.6.3.0	201.1.7.2

Router R2

Destination Network	*Next Router*
73.16.4.0	
201.1.7.0	
11.72.3.0	
201.1.6.0	
88.33.5.0	
14.6.3.0	

Router R3

Destination Network	*Next Router*
73.16.4.0	
201.1.7.0	201.1.6.2
11.72.3.0	
201.1.6.0	
88.33.5.0	
14.6.3.0	Direct

Router R4

Destination Network	*Next Router*
73.16.4.0	11.72.3.5
201.1.7.0	
11.72.3.0	
201.1.6.0	88.33.5.32
88.33.5.0	
14.6.3.0	

Question 5 [13 marks]

From the figure for Question 4, assume a firewall is used on Router R1, which controls access to the internal network of with computers C1 and C2 (that is, Computers C1 and C2 is "inside", while all other routers and computers are "outside").

Notes and hints:

- You do not have to use all rows in the tables (and you can add more rows if needed).
- You can assume that the tables are the FORWARD tables as used by `iptables`.
- Use '*' to indicate the value is not specified (or any value can be used).
- You must specify the interface that the packet arrives by either INSIDE (meaning IP 73.16.4.1) or OUTSIDE (meaning 201.1.7.3 and/or 11.72.3.5).
- Although only 3 computers are shown (C1, C2 and C3), you should assume that there may be other computers on each network (e.g. more than two computers on the "inside" network).
- Some entries are already given – you cannot change those entries.

a) Add entries to the following firewall tables to implement the required policy. You should assume the default policy is to ACCEPT packets.

i. Drop all traffic to and from Computer C1 [3 marks]

Arrives on Interface (-i)	IP source (-s)	Port source (--sport)	IP dest (-d)	Port dest (--dport)	Protocol (-p)	Action (-j)
INSIDE	73.16.4.2	*	*	*	*	DROP

ii. Block the "inside" network from initiating or responding to PINGs (and other ICMP traffic) to computers "outside". [3 marks]

Arrives on Interface (-i)	IP source (-s)	Port source (--sport)	IP dest (-d)	Port dest (--dport)	Protocol (-p)	Action (-j)

iii. Block access to the web server on Computer C2 from any "outside" computer/router. [3 marks]

Arrives on Interface (-i)	IP source (-s)	Port source (--sport)	IP dest (-d)	Port dest (--dport)	Protocol (-p)	Action (-j)

b) If you assume that the default policy is DROP (instead of ACCEPT in part (a)), then complete the firewall table to block all traffic, except traffic between any outside computer and a web server on Computer C2. Hint: make sure you consider the return traffic from web server to other computers. [4 marks]

Arrives on Interface (-i)	IP source (-s)	Port source (--sport)	IP dest (-d)	Port dest (--dport)	Protocol (-p)	Action (-j)

Question 6 [20 marks]

6.1 The difference between a host and router on Linux is that:

a) A router has a routing table, but a host does not have a routing table
b) A host will forward packets, but a router will not forward packets
c) A host has a routing table, but a router does not have a routing table
d) A router will forward packets, but a host will not forward packets
e) A router can have multiple network (LAN) cards, but a host can only have one network (LAN) card
f) A host can be a destination of a packet, whereas a router cannot be a destination of a packet

6.2 If you edit the file `/proc/sys/net/ipv4/ip_forward` and set the value to 1, then what is the effect:

a) Sets the IP address of the computer to 1
b) Enables the computer to act as a router
c) Forces the computer to never forward packets
d) Sets the computer to use IP version 4 (instead of IP version 6)
e) Forces an IP packet to be sent containing the message "1"
f) None of the above.

6.3 The following Linux command is issued on a router with IP address 192.168.2.3. It adds a routing table entry that indicates that:

```
route add –net 192.168.1.0 netmask 255.255.255.0 gw 192.168.2.1 dev eth1
```

a) Packets destined to host 192.168.1.0 will be sent via Ethernet interface eth1
b) Packets destined to host 192.168.1.3 will be sent to host 192.168.1.0
c) Packets destined to host 192.168.1.3 will be sent to host 192.168.1.1
d) Packets destined to host 192.168.2.1 will be sent to host 192.168.1.0
e) Packets destined to host 192.168.1.3 will be sent via Ethernet interface eth1

6.4 In a client/server application, how does the server know the port number that the client is using?

a) The client port number is a well-known port
b) The client port number is the same as the server port number
c) The server does not need to know the client port number
d) The client port number is included in the initial TCP SYN sent to the server
e) The server chooses a random port number for the client to use

6.5 What is the purpose of the TCP three-way handshake?

a) To verify the source and destination IP addresses
b) To obtain the destination IP address of the server
c) To synchronize sequence numbers prior to data transmission
d) To determine the number of bytes that will be sent to the server
e) To agree upon the speed at which data will be sent between source and destination

6.6 What items uniquely identify a connection between a client and server application on the Internet:

a) Client IP address; Client Port number; Server IP address; Server Port number
b) Client MAC address; Server MAC address
c) Client IP address; Server IP address
d) Client MAC address; Client IP address; Server MAC address; Server IP address
e) Client Port number; Server port number

6.7 What does the C function `inet_ntoa()` do:

a) Converts an Internet address structure to a string
b) Obtains the address of the client that connected to the server
c) Converts an Internet address represented as a string to an Internet address structure
d) Obtains the address being used by the server
e) Uses DNS to obtain the IP address for a domain name

6.8 A computer is running a web (HTTP) server, FTP server and email (SMTP) server, and receives a packet from a client computer. What does the operating system use to identify the application to which the packet should be sent to for processing?

a) Email address
b) Port number
c) Domain name (URL)
d) MAC address
e) IP address
f) None of the above

6.9 What does this Linux command do on computer A (assume the default firewall policy is to accept packets)?

```
iptables –A INPUT –s 192.168.1.3 –p tcp –-dport 80 –j DROP
```

a) Drops all TCP packets sent from computer A to the web server on the computer with IP address 192.168.1.3
b) Drops all TCP packets sent from the computer with IP address 192.168.1.3 to the web server on computer A
c) Drops all TCP packets sent from computer A to the computer with IP address 192.168.1.3
d) Drops all TCP packets sent from the computer with IP address 192.168.1.3 to computer A

6.10 If you wanted to configure the SIIT gateway router/firewall to drop all ICMP (Ping) packets from SIIT PCs to any server on the Internet, what chain in `iptables` would you use?

a) INPUT
b) OUTPUT
c) FORWARD
d) The router/firewall cannot be configured to drop ICMP packets, even by a network administrator

Question 7 [6 marks]

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

```
61.19.242.176 - - [05/Mar/2008:08:21:52 +0700] "GET /dir1/index.html HTTP/1.0"
200 1220 "-" "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/Mar/2008:08:21:53 +0700] "GET /dir1/main.css HTTP/1.0"
200 434 "http://sandilands.info/dir1/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/Mar/2008:08:21:59 +0700] "GET /dir1/page1.html HTTP/1.0"
200 13354 "http://sandilands.info/dir1/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/Mar/2008:08:23:05 +0700] "GET /dir1/file2.txt HTTP/1.0"
200 581 "http://sandilands.info/dir1/page1.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/Mar/2008:08:23:21 +0700] "GET /dir1/page3.html HTTP/1.0"
200 1697 "http://sandilands.info/dir1/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/Mar/2008:08:23:45 +0700] "GET /dir1/page4.html HTTP/1.0"
404 368 "http://sandilands.info/dir1/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/Mar/2008:08:24:22 +0700] "GET /dir1/page5.html HTTP/1.0"
200 2303 "http://sandilands.info/dir1/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"
```

Answer the following questions based on the above information.

7.1 How many bytes is the file `http://sandilands.info/dir1/index.html`?

a) 200
b) 368
c) 404
d) 434
e) 1220
f) The file does not exist
g) None of the above

7.2 How many bytes is the file `http://sandilands.info/dir1/page4.html`?

a) 200
b) 368
c) 404
d) 434
e) 1220
f) The file does not exist
g) None of the above

7.3 Which of the following is most likely to be false?

a) There are at least four links to other pages on http://sandilands.info/dir1/index.html
b) The person on 61.19.242.176 is using Firefox web browser on the Windows operating system
c) The person on 61.19.242.176 typed the address http://sandilands.info/dir1/index.html into the address bar of their web browser (as opposed to clicking on a link to this page)
d) The pages browsed on sandilands.info are protected by HTTP authentication.