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

Sirindhorn International Institute of Technology
Thammasat University

Final Examination: Semester 2/2006

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

Instructor : Dr Steven Gordon

Date/Time : 7 March 2007, 13:30 to 16:30 (3 hours)

Instructions:

- This examination paper has 14 pages (including this page).
- Condition of Examination
  Closed book (No dictionary, No calculator allowed)
- 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.

Part A – Multiple Choice [26 marks]

Select the most accurate answer. Only select one answer. Each question is worth 2 marks.

1. The C function `gethostbyname()`:
   a) Uses ARP to obtain the hardware address for a corresponding IP address
   b) Uses DNS to obtain the IP address of a host name
   c) Uses HTTP to obtain the address of the web server
   d) Returns the IP address of the client that connected to a server
   e) Returns the IP address of a server that responded to a client
   f) Returns the hardware address of the client that connected to a server
   g) Returns the hardware address of a server that respond to a client

2. The difference between a host and router on Linux is that:
   a) A router will forward packets, but a host will not forward packets
   b) A host will forward packets, but a router will not forward packets
   c) A router has a routing table, but a host does not have a routing table
   d) A host has a routing table, but a router does not have a routing table
   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

3. The purpose of the following C code on a server is to:

```
address.sin_family = AF_INET;
address.sin_addr.s_addr = INADDR_ANY;
address.sin_port = htons(port);
```

   a) Obtain the IP address of a server using DNS
   b) Format the IP address of this host (as well as port number) into a structure used by sockets
   c) Manually convert the domain name of the server to an IP address (without using DNS)
   d) Retrieve the IP address of the client that has connected to the server

4. What does this Linux command do:

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

   a) Sets the IP address of the computer to 1
   b) Prints the string "1 > /proc/sys/ent/ipv4/ip_forward" to the screen
   c) Enables the computer to act as a router
   d) Forces the computer to never forward packets
   e) Sets the computer to use IP version 4 (instead of IP version 6)
   f) Forces an IP packet to be sent containing the message "1"

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

7. What protocol is used if the following socket C code is used:

```
sockfd = socket(AF_INET, SOCK_STREAM, 0);
```

   a) DNS
   b) ICMP
   c) UDP
   d) TCP
   e) HTTP
   f) FTP

8. What is the purpose of the TCP three-way handshake?
   a) To obtain the destination IP address of the server
   b) To determine the number of bytes that will be sent to the server
   c) To verify the source and destination IP addresses
   d) To agree upon the speed at which data will be sent between source and destination
   e) To synchronize sequence numbers prior to data transmission

9. 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

10. What does the C function `inet_ntoa()` do:
   a) Obtains the address of the client that connected to the server
   b) Converts an Internet address structure to a string

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

11. 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) Domain name (URL)
    c) MAC address
    d) Port number
    e) IP address

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

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

Part B – General Questions [64 marks]

Question 1 [17 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>
```

a) Explain what the above configuration changes do. [4 marks]

When a file in the /var/www/private (or by URL, http://www.example.com/private/) directory is requested from a client (web browser), user authentication will be required. The username supplied must be siit and the corresponding password is stored in the file /etc/apache2/passwd/passwords.

b) In addition to changing the above configuration, you may use the `htpasswd` command. What do you use `htpasswd` for? [2 marks]

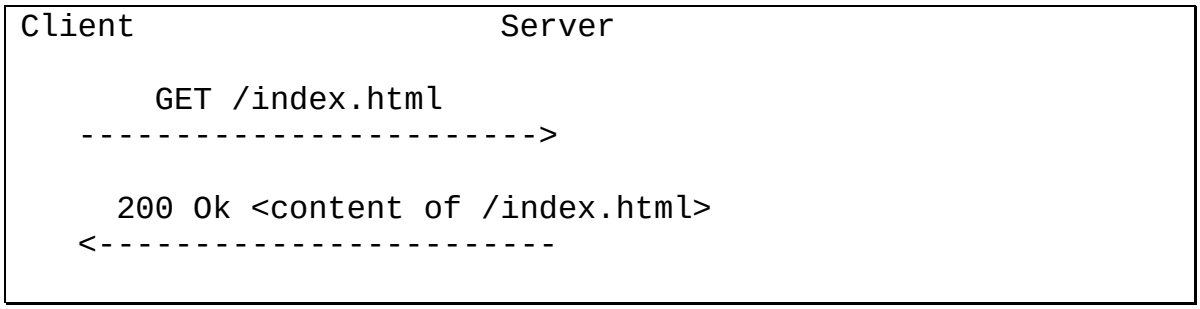
htpasswd is used to generate the username and passwords used for authentication.

c) Assuming the files `/var/www/index.html`, `/var/www/private/page.html` and `/var/www/private/anotherpage.html` exist on the web server, draw a time sequence diagram that shows the exchange of HTTP messages between a web browser and server when:

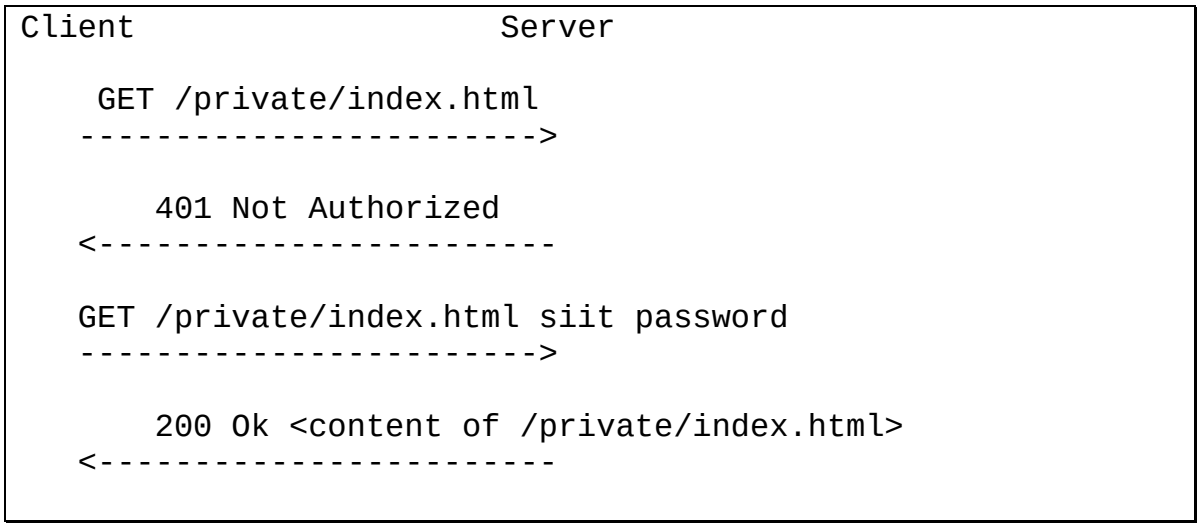
   i. The user (of the web browser) browses to http://www.example.com/index.html [3 marks]
   ii. The user browses to http://www.example.com/private/index.html for the first time. [5 marks]

Make sure you show or describe the type of messages that are sent, as well as any important information included in the messages.

Time Sequence Diagram for Part (i)



Time Sequence Diagram for Part (ii)



d) If, after part (c), the user browses to http://www.example.com/private/anotherpage.html, then does the web browser send a request to the server if:
   i. The web browser does not cache web pages and does not cache user name/passwords [1 mark, circle the answer] *YES*

   ii. The web browser does not cache web pages, but does cache user name/passwords [1 mark, circle the answer] *YES*

e) In part (c)(ii), if another third computer (e.g. a router between client and server) intercepted the exchange of HTTP messages, can the third computer obtain the web users password? [1 mark, circle the answer] *YES*

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()

_connect_____ triggers a TCP SYN segment to be sent

_write______ may trigger a TCP data segment to be sent

_bind_____ associates an IP address and port number to a socket

_socket______ creates an endpoint for communication with another computer

_accept______ blocks until a TCP SYN segment is received

_read_____ blocks until a TCP data segment is received

_listen______ marks a socket as able to accept connections

Question 3 [10 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);
      }
}
```

a) Is the `accept()` function blocking or non-blocking? [1 mark, circle the answer]

BLOCKING

b) Explain what your answer to part (a) means with respect to the `accept()` function. [2 marks]

The accept() function will not return (i.e. it blocks) until the computer receives a TCP SYN segment (to initiate a connection), or until an error occurs.

c) With respect to how the server works, explain the purpose of using `fork()` in this code segment. [3 marks]

The function fork() creates a new child process of the currently executing program (process). Then we have two server processes: one to handle new connections (it completes the while loop and goes back to accept()) and another to handle the request for this connection.

d) Assuming there are no errors, does the parent server process call the `handlerequest()` function? [1 mark, circle the answer]

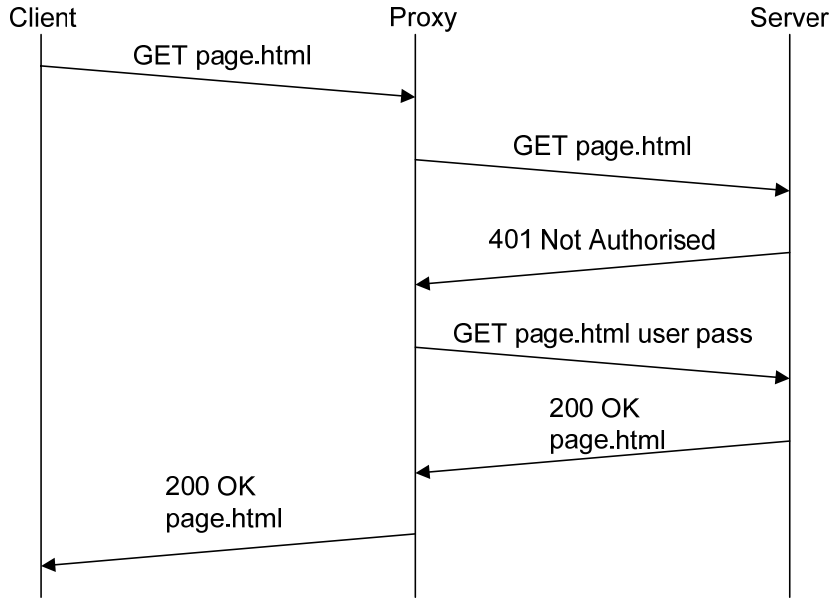
NO

e) If the `handlerequest()` function takes 10 seconds to execute, can a second client connect to the server before the function completes? Explain your answer. [3 marks]

Yes. Since we have fork'ed a new child process to handle the request, the parent server process can receive a second (and any subsequent) connection. That is, the accepting of connections and handling of the request can occur in parallel.

Question 4 [6 marks]

Assume your client retrieves web pages from a simple server, similar to that in Assignment 2. However, you have created your own proxy server that will store your usernames and passwords for different sites. That is, a request for a page is sent from client to proxy, the proxy then sends the request to the server. If the server responds with "401 Not authorized", then the proxy will re-send the request with the correct username and password. Using the proxy means the client does not have to prompt for passwords (instead the usernames and passwords are managed by the proxy). The time sequence diagram below shows an example set of messages:



a) We can classify the proxy as both a "client" program and "server" program. Explain why. [3 marks]

The proxy must act as a server, in terms of waiting for requests from a client (listens, accepts, etc.). Hence the proxy must run on a port known by the client. However, once a request is received from the client the proxy initiates a connection to the real server – hence in this process the proxy is acting also as a client.

b) Explain one method in which the proxy knows where to send the GET request it receives from the client (that is, how does it know where to send "GET page.html"?). [3 marks]

The client can include the IP address or URL of the real server in the GET request. Therefore when the proxy receives the GET request, the proxy will know where to send the request.

Question 5 [11 marks]

The figure on page 12 shows a computer network with 3 computers, 3 routers and 1 switch. Each device is labelled with a unique letter (A to G), and the network interface (IF) of each device is labelled with a number (e.g. IF1, IF2). E2 refers to interface (IF) 2 on device E (a router). From the figure, answer the following questions.

a) How many different IP networks are used? [1 mark]

4

b) Complete the following table showing the interface configurations: [6.5 marks]

Device	**Interface**	**IP address**	**Subnet mask**	**Default gateway**
Computer A	IF1	192.168.3.7	255.255.255.0	192.168.3.2
Computer B	IF1	*192.168.3.x*	*255.255.255.0*	*192.168.3.2*
Computer C	IF1	*200.1.2.y*	*255.255.255.0*	*200.1.2.1*
Router E	IF1	*192.168.3.2*	*255.255.255.0*	not applicable
	IF2	*a.b*	255.255.0.0	not applicable
Router F	IF1	*a.c*	*255.255.0.0*	not applicable
	IF2	*172.16.z*	*255.255.0.0*	not applicable
Router G	IF1	172.16.12.1	255.255.0.0	not applicable
	IF2	200.1.2.1	255.255.255.0	not applicable

c) Based on the addresses configured in part (c), complete the routing tables for each router (hint: the "Next Router" for the first entry of Router E will be the IP address of IF1 on Router F): [3.5 marks]

Router E

Destination Network	**Destination Subnet Mask**	**Next Router**
200.1.2.0	255.255.255.0	*a.c*
172.16.0.0	255.255.0.0	*a.c*

Router F

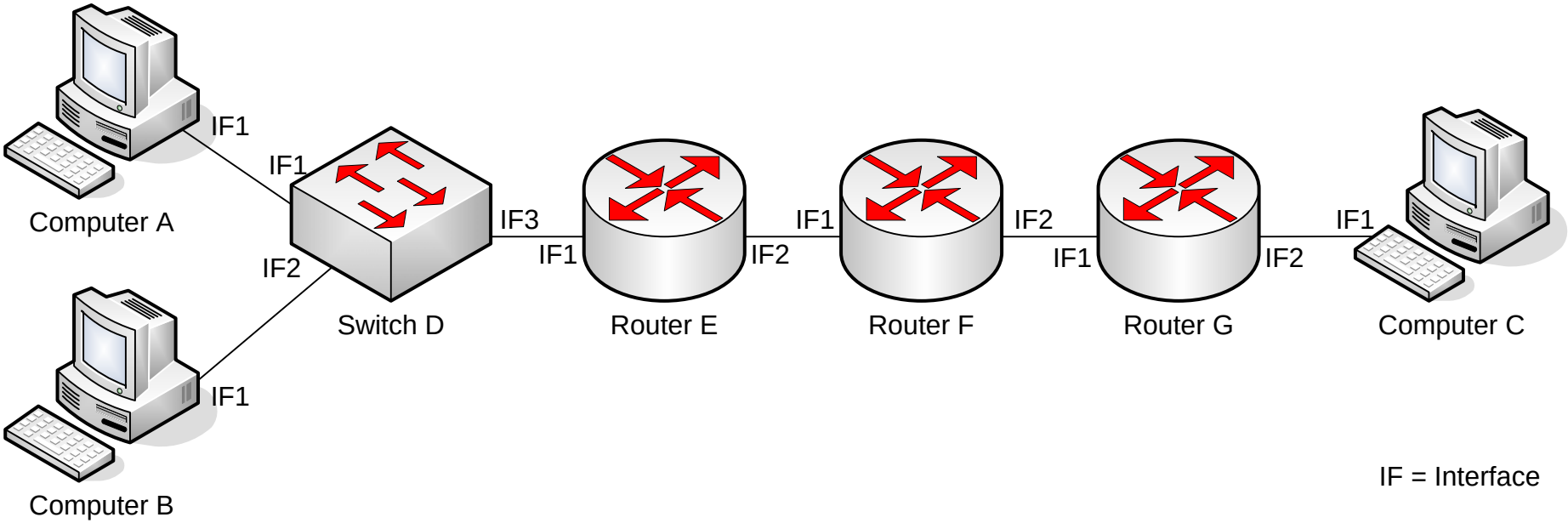
Destination Network	**Destination Subnet Mask**	**Next Router**
200.1.2.0	255.255.255.0	172.16.12.1
192.168.3.0	255.255.255.0	*a.b*

Router G

Destination Network	**Destination Subnet Mask**	**Next Router**
192.168.3.0	255.255.255.0	*172.16.z*
a.0.0	*255.255.0.0*	*172.16.z*

Explanation:
In this question you could give different possible IP addresses as answers in some cases. I have shown them as a.b, a.z, x, y etc.
a.b means a is the network portion of the address and b is the host portion. Example addresses could be: x=3, y=2, a=172.15, b=1.1, c=1.2 and z=12.2.

Figure for Questions 5 and 6



Question 6 [13 marks]

From the figure for Question 5, assume a firewall is used on Router G, which controls access to the internal network of Computer C (that is, Computer C 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`.
- You must specify the interface that the packet arrives on.
- Use '*' to indicate the value is not specified (or any value can be used).
- You can use the IP addresses you selected in Question 5. However, if you did not complete Question 5, then simply refer to the Device and Interface in the IP address field, e.g. "Computer A, IF1".
- Although only 3 computers are shown (A, B and C), you should assume that there may be other computers on each network (e.g. more than one computer on the "inside" network).

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 A [3 marks]

Arrives on Interface (-i)	IP source (-s)	Port source (--sport)	IP dest (-d)	Port dest (--dport)	Protocol (-p)	Action (-j)
IF1	*192.168.3.7*	*	*	*	*	*DROP*
IF2	*	*	*192.168.3.7*	*	*	*DROP*

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

Arrives on Interface (-i)	IP source (-s)	Port source (--sport)	IP dest (-d)	Port dest (--dport)	Protocol (-p)	Action (-j)
IF1	*	*	*	*	*icmp*	*DROP*
IF2	*	*	*	*	*icmp*	*DROP*

Explanation: in fact, just one of the above rules would be sufficient to block Pings, as only dropping a request or response is sufficient to stop Ping working

iii. Block access to the web server on Computer C 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)
IF1	*	*	*200.1.2.y*	*80*	*tcp*	*DROP*

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 C. 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)
IF1	*	*	*200.1.2.y*	*80*	*tcp*	*ACCEPT*
IF2	*200.1.2.y*	*	*	*	*tcp*	*ACCEPT*

In fact, the port source in the second row should be limited to only client ports, e.g. > 1023.