Name …..ID …............................. Section …........Seat No..........
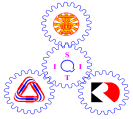
Sirindhorn International Institute of Technology
Thammasat University

Final Examination Answers: Semester 2/2008

Course Title : ITS332 Information Technology II Laboratory

Instructor : Dr Steven Gordon

Date/Time : Friday 6 March 2009, 13:30 to 16:30

Instructions:

- This examination paper has 13 pages (including this page).

- Condition of Examination
  Closed book
  No dictionary
  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.

- 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.

- If a question requires an IP address for an answer, then you may select any valid IP address that satisfies all conditions of the question.

- Assume 8 bits = 1 Byte; 1000 Bytes = 1KB; 1000KB = 1MB; 1000MB = 1GB; ...

Question 1 [5 marks]

The following shows portion of an example log from Apache web server 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 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/Mar/2008:08:21:53 +0700] "GET /dir1/main.css HTTP/1.0" 200
540 "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"
200 906 "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 1100 "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 2056 "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"
404 204 "http://sandilands.info/dir1/page3.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/page3.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.

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

    a) 200

    b) 204

    c) 404

    d) 540

    e) 906

    f) 1100

    g) 1200

    h) The file does not exist on the server

    i) None of the above

2. How many bytes is the file http://sandilands.info/dir1/file2.txt?

    a) 200

b) 204

c) 404

d) 540

e) 906

f) 1100

g) 1200

h) The file does not exist on the server

i) None of the above

3. What protocol version is used by the web browser to retrieve pages?

a) 1.0

b) 1.8.1.12

c) 2.0.0.12

d) 5.0

e) 5.1

f) None of the above

4. 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 probably used the "Back" button, and explain why/how it shows this. [2 marks]

Answer

The user visited page1.html, via the index.html, (3rd entry) and then clicked on a link to file2.txt (4th entry). The next (5th) entry shows the user clicked on a link to page3.html via the index.html. This suggests the user went "Back" from file2.txt to page1.html to index.html.

Question 2 [6 marks]

1. What items uniquely identify a TCP connection between an email client and an email server? [2 marks]

Answer

Client IP address, client port number, server IP address, server port number

When starting a server program, you usually must give the port number (either as a command line option or in a configuration file). Whereas when starting a client program, you do not specify the port of the client.

2. Explain why you must give the port number of the server when starting the server program. [2 marks]

Answer

Because the port number must be known by the client, and hence cannot be chosen randomly. The user chooses the port number and informs the client.

3. Does the client use a port number? If no, why not. If yes, when/how is it assigned? [2 marks]

Answer

Yes. The operating system assigns the port number from a set of unused ports.

Question 3 [9 marks]

The following code shows an example UDP client and UDP server (that is, a client and server that use UDP to communicate).

UDP-based sockets communications often uses the `sendto()` and `recvfrom()` functions (rather than `send()` and `recv()`). These functions include an additional 3 parameters: the first is for flags (usually 0); the second is the address of the other end-point; and the third is the length of the address structure.

As UDP is not connection-oriented, there is no need for the client or server to establish the connection with sockets function calls. Instead, the destination address is specified for every datagram that is sent.

The following is `client.c` (header includes are omitted):

```c
int main(int argc, char *argv[])
{
    int sock, n;
    struct sockaddr_in server, from;
    struct hostent *hp;
    char buffer[256],datagram[256];
    size_t addrlength;

    if (argc != 3) {
        printf("Usage: server port\n");
        exit(1);
    }

    sock= socket(AF_INET, SOCK_DGRAM, 0);
    server.sin_family = AF_INET;
    hp = gethostbyname(argv[1]);

    /* Set the server address and port */
    bcopy((char *)hp->h_addr, (char *)&server.sin_addr, hp->h_length);
    server.sin_port = htons(atoi(argv[2]));

    addrlength=sizeof(struct sockaddr_in);

    printf("Please enter the message: ");
    bzero(buffer,256);
    fgets(buffer,255,stdin);

    n=sendto(sock,buffer,strlen(buffer),
            0,(struct sockaddr *) &server,addrlength);

    n = recvfrom(sock,buffer,256,
                0,(struct sockaddr *) &from, &addrlength);
    strncpy(datagram,buffer,n);
    printf("Received response: %s",datagram);
}
```

The following is `server.c` (header includes are omitted):

```
int main(int argc, char *argv[])
{
   int sock, length, n;
   struct sockaddr_in server;
   struct sockaddr_in from;
   char buf[1024], datagram[1024];
   size_t fromlen;

   if (argc < 2) {
      fprintf(stderr, "ERROR, no port provided\n");
      exit(0);
   }

   sock=socket(AF_INET, SOCK_DGRAM, 0);

   length = sizeof(server);
   bzero(&server,length);

   /* Set the server address */
   server.sin_family=AF_INET;
   server.sin_addr.s_addr=INADDR_ANY;
   server.sin_port=htons(atoi(argv[1]));

   if (bind(sock,(struct sockaddr *)&server,length)<0)
       error("binding");

   fromlen = sizeof(struct sockaddr_in);

   while (1) {
      n = recvfrom(sock,buf,1024,
                  0,(struct sockaddr *)&from,&fromlen);
      strncpy(datagram,buf,n)
      printf("Received datagram: %s\n",datagram);
      n = sendto(sock,"Got your message\n",17,
                  0,(struct sockaddr *)&from,fromlen);
   }
 }
```

Assume the server is to run on 203.16.78.3, using port 4034, and the client is to run on 72.45.103.1.

1. What is the command (including options) to start the server? [1 mark]

Answer
server 4034

2. What is the command (including options) to start the client? [1 mark]

Answer
client 203.16.78.3 4034

3. Assume the user at the client types in "Hello" when prompted. What is the output shown at the client? (That is, what is all the text displayed in the terminal after the client completes) [2 marks]

Answer
Please enter the message:
Hello

Received response: Got your message

4. What is the output shown at the server? [1 mark]

Answer
Received datagram: Hello

5. Explain how the server knows the address of the client (refer to the line(s) of code). [2 marks]

Answer
In the `recvfrom()` function when receiving a datagram, the server places the source IP address (i.e. the clients) in the `from` variable.

6. Assume the server 203.16.78.3 also had the domain name `server.example.com`. The `client.c` program will work if the user at the client uses the IP address or the domain name. What line(s) of code allow this to work? [2 marks]

Answer
The `gethostbyname()` function takes the input from the user and converts to an IP address (using DNS) if necessary/possible.

Question 4 [8 marks]

Consider the C socket functions. Write the function name in the blank space which best meets the description. Only give one function per description, but you may use a function multiple times.

1. Associates an IP address with a socket   _____

2. Creates an end-point for communication   _____

3. Blocks until a packet is received   _____

4. Causes a TCP SYN segment to be sent   _____

5. Tells a server to listen for connections   _____

6. Returns a new socket identifier after receiving TCP SYN   _____

7. Sends application data to the TCP software in the OS   _____

8. Returns the number of bytes successfully received   _____

Answers

1. bind

2. socket

3. accept or read

4. connect

5. listen

6. accept

7. write

8. read

Question 5 [7 marks]

Answer the questions about the following example code segment for a server program (lines of code are given on the left):

```
1. while (1) {
2.         newsockfd = accept(sockfd, (struct sockaddr *) &address, &len);
3.         if (newsockfd < 0) error("ERROR on accept");
4.         pid = fork();
5.         if (pid < 0) error("ERROR on fork");
6.         if (pid == 0)  {
7.                 close(sockfd);
8.                 handlerequest(newsockfd);
9.                 exit(0);
10.        }
11.        else {
12.                close(newsockfd);
13.        }
14. }
```

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

1. Does the server know the address of the client *before* this code segment executes (that is, before line 1)? Explain your answer. [1 mark]

Answer

No. The server obtains the clients address when accept() returns.

2. What does `fork()` do? [1 mark]

Answer

Creates a copy of the current executing process.

3. What is the value of `pid` in the parent server? [1 mark]

Answer

The process ID assigned by the OS to the child.

4. What is the value of `pid` in the child server? [1 mark]

Answer

0

5. When does the parent server program exit? Explain your answer or refer to the line of code. [1 mark]

Answer

It doesn't. The parent server enters an infinite loop

6. When does the client server program exit? Explain your answer or refer to the line of code. [1 mark]

Answer

Line 9. After it has handle the request.

7. How many clients can connect to the server at the same time? Explain your answer. [1 mark]

Answer

There is no limit specified. It is only limited by memory on the computer (or other options not shown in the code segment).

Question 6 [10 marks]

A selection of options available with the program `iptables` include:

```
-s source          -d destination      -p protocol
-i inputinterface  -o outputinterface -A chain
--sport sourceport --dport destport    -j action
```

Consider `iptables` running on a R2 in the network below, with the internal networks to the left of the firewall. Note that although the figure only shows 7 hosts in total, you must assume there may be many hosts (hence design your firewall rules to support any number of hosts).
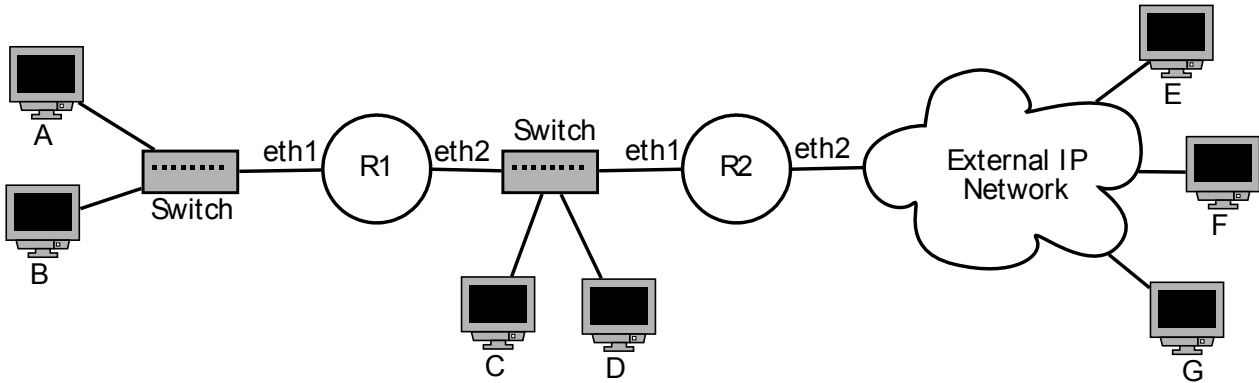

Figure 1: Firewall Network

The IP addresses are given in the table below (assume subnet mask of /24 for all addresses):

Host/Interface	IP Address	Host/Interface	IP Address
A	72.16.34.2	R2/eth1	80.0.7.1
B	72.16.34.3	R2/eth2	63.50.5.2
R1/eth1	72.16.34.1	E	101.23.6.1
R1/eth2	80.0.7.2	F	112.6.76.5
C	80.0.7.3	G	123.87.44.7
D	80.0.7.4	-	-

Assume the default policy of iptables is ALLOW.

Write the `iptables` command (or commands) to perform the following operations:

1. Block all PING requests coming from the external networks in to the internal networks. [2 marks]

Answer

iptables -A FORWARD -i eth2 -p icmp -j DROP

iptables -A INPUT -i eth2 -p icmp -j DROP

2. Block all web traffic from internal hosts to the web server on computer F. [2 marks]

Answer

```
iptables -A FORWARD -p tcp -d 112.6.76.5 --dport 80 -j DROP
```

Now assume the previous commands have been flushed, and the default policy is set to DROP.

3. Allow internal hosts to access all external web servers, except the web server on computer F. [3 marks]

Answer

iptables -A FORWARD -p tcp -d 112.6.76.5 --dport 80 -j DROP

iptables -A FORWARD -p tcp --dport 80 -j ALLOW

iptables -A FORWARD -p tcp --sport 80 -j ALLOW

4. Allow computer G to PING the firewall (and the firewall to respond). [3 marks]

Answer

iptables -A INPUT -p icmp -s 123.87.44.7 -j ALLOW

iptables -A OUTPUT -p icmp -d 123.87.44.7 -j ALLOW

Question 7 [5 marks]

1. Draw a diagram that illustrates the exchange of HTTP messages between a browser and server assuming the requested file exists on the server but requires authentication (that is, is password protected by the Apache web server). You may assume the web browser user knows the correct username/password if prompted. For each message, you must clearly show the information included in the request, as well as the status code include in the response (you don't have to show the exact HTTP message format, only the useful information for the question). Assume no caching is used. [4 marks]

Possible status codes: 200 Ok   304 Not Modified

401 Unauthorized   404 Not Found

Answer

GET file ----->

<------- 401 Unauthorized

GET file username password ---->

<------- 200 Ok

2. On your diagram, identify when the user is prompted for a password by the web browser. [1 mark]

Answer

After the 401 response is received.