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

Sirindhorn International Institute of Technology
Thammasat University

Final Examination: Semester 2/2009

Course Title : ITS332 Information Technology II Laboratory

Instructor : Dr Steven Gordon

Date/Time : Tuesday 9 March 2010, 9:00 to 10:30

Instructions:

- This examination paper has 11 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.
- Assume 8 bits = 1 Byte; 1000 Bytes = 1KB; 1000KB = 1MB; 1000MB = 1GB; ...

Questions [50 marks]

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.

```
72.33.16.102 - - [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:2.9.2.12) Gecko/20100201 Firefox/3.5"

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"

43.17.110.3 - - [05/Mar/2008:08:22:24 +0700] "GET /dir1/page1.html HTTP/1.0" 200 906 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:2.9.2.12) Gecko/20100201 Firefox/3.5"

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"

43.17.110.3 - - [05/Mar/2008:08:23:18 +0700] "GET /dir1/page3.html HTTP/1.1" 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/2008:08:23:21 +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"

72.33.16.102 - - [05/Mar/2008:08:23:30 +0700] "GET /dir1/page1.html HTTP/1.0" 401 254 "http://sandilands.info/dir1/index.html" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:2.9.2.12) Gecko/20100201 Firefox/3.5"

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"

43.17.110.3 - - [05/Mar/2008:08:23:59 +0700] "GET /dir1/page4.html HTTP/1.1" 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"

43.17.110.3 - - [05/Mar/2008:08:24:22 +0700] "GET /dir1/page5.html HTTP/1.1" 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. What is the address of the computer that requested `dir1/page1.html` but was not authorised to access the page? [1 mark]

2. What is the size of `/dir/page1.html`? [1 mark]

3. What protocol version is used by the web browser on 43.17.110.3 to retrieve pages? [1 mark]

4. Does `/dir1/page3.html` contain links to other pages? If so, which other pages? If not, why not? [1 mark]

5. Do you think the browser on 61.19.242.176 visited `/dir1/index.html`? Explain your answer. [1 mark]

Question 2 [4 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. If a user using a web browser enters the address `http://www.example.com/index.html`:
   a) The server will check the file `/etc/apache2/passwd/passwords` to determine if the browser has sent the correct username/password
   b) The user will be prompted for a username/password by their web browser
   c) 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
   d) A 404 Not Found will be returned by the server
   e) The first HTTP request sent from the browser to server will contain the user's username/password
   f) None of the above.

2. If a user enters the address `http://www.example.com/private/index.html` in a browser:
   a) A 404 Not Found will be returned by the server
   b) 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
   c) The first HTTP request sent from the browser to server will contain the user's username/password
   d) The user will be prompted for a username/password by their web browser
   e) None of the above.

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

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 3 [27 marks]

Consider the code in client.c and server.c below. This is similar to the example client and server provide in the lab. The header includes and some error checking code is not shown. Answer the questions based on this code only.

client.c

```
1. int main(int argc, char *argv[])
2. {
3.     int sockfd, b, n;
4.     struct sockaddr_in addr;
5.     struct hostent *server;
6.     char a[256];
7.     b = atoi(argv[2]);
8.    sockfd = socket(AF_INET, SOCK_STREAM, 0);
9.     server = gethostbyname(argv[1]);
10.    bzero((char *) &addr, sizeof(addr));
11.    addr.sin_family = AF_INET;
12.    bcopy((char *)server->h_addr,
13.         (char *)&addr.sin_addr.s_addr,
14.         server->h_length);
15.    addr.sin_port = htons(b);
16.    if (connect(sockfd,(struct sockaddr *) &addr,sizeof(addr))< 0)
17.        error("ERROR connecting");
18.    printf("Please enter the message: ");
19.    bzero(a,256);
20.    fgets(a,255,stdin);
21.    n = write(sockfd,a,strlen(a));
22.    bzero(a,256);
23.    n = read(sockfd,a,255);
24.    printf("%s\n",a);
25.    return 0;
26. }
```

server.c

```
27. int main(int argc, char *argv[])
28. {
29.     int sockfd, newsockfd;
30.     int a;
31.     int p;
32.     struct sockaddr_in addr1, addr2;
33.     size_t b;
34.     int n;
35.     char m[256];
36.     sockfd = socket(AF_INET, SOCK_STREAM, 0);
37.     bzero((char *) &addr1, sizeof(addr1));
38.     a = atoi(argv[1]);
39.     addr1.sin_family = AF_INET;
40.     addr1.sin_addr.s_addr = INADDR_ANY;
41.     addr1.sin_port = htons(a);
42.     if (bind(sockfd, (struct sockaddr *) &addr1, sizeof(addr1))<0)
43.              error("ERROR on binding");
44.     listen(sockfd,5);
45.     b = sizeof(addr2);
46.     while (1) {
47.         newsockfd = accept(sockfd, (struct sockaddr *) &addr2, &b);
48.         p = fork();
49.         if (p < 0)
50.             error("ERROR on fork");
```

```
51.         if (p == 0)  {
52.                close(sockfd);
53.                bzero(m,256);
54.                n = read(newsockfd,m,255);
55.                printf("Here is the message: %s\n",m);
56.                n = write(newsockfd,"I got your message",18);
57.                exit(0);
58.         }
59.         else close(newsockfd);
60.     }
61.     return 0;
62. }
```

1. Give the number of the line of code that implements the following functionality (give only one line number, although there may be more than one correct answer): [15 marks]
   a) Triggers the sending of a TCP SYN segment to the server. Line:
   b) Converts the port number given on server command line into an integer. Line:
   c) Blocks until a TCP SYN segment is received. Line:
   d) Closes a child process at the server. Line:
   e) Associates an IP address with a socket. Line:
   f) Receives the text (via TCP) that the user typed in at the client. Line:
   g) Parent server process that closes a socket. Line:
   h) Obtains an IP address if a domain name was entered. Line:
   i) Blocks the client until a TCP segment containing data is received. Line:
   j) Creates an end-point for communication. Line:
   k) Tells the server to listen for connections. Line:
   l) Returns the number of bytes successfully received by the client. Line:
   m) Creates a child process. Line:
   n) Never executes if the server is always running. Line:
   o) Puts the IP address of the client into a variable. Line:

2. What command would you use to compile the server source code to produce an executable called `myserver`? [1 mark]

3. What command would you use to run the server? [1 mark]

4. How many input parameters does the client take? Explain the meaning of all input parameters. [2 marks]

5. If after the client and server are running, the user at the client types in “My name is steve”, what is displayed on the screen at the server? [1 mark]

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

7. Once the client and server are running, what items uniquely identify a connection between the client and server? [2 marks]

8. If you wanted to modify the client so that the message to be sent is a word entered as an additional command line argument (instead of prompting the user), explain what changes you would make to `client.c`. State the lines you would delete/modify, and give the new code you would add and the location you would add them (e.g. “Add the following code after line 3”). [2 marks]

9. If you wanted to modify the server so that it only receives 20 bytes from the client, explain what changes you would make to `server.c`. [2 marks]

Question 4 [5 marks]

For the following cases you need to draw a diagram that illustrates the exchange of HTTP messages between a browser and server. 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.

Possible status codes:	200 Ok	304 Not Modified
	401 Unauthorized	404 Not Found

1. Assume the file requested (`file1.html`) does not exist on the server. [2 marks]

2. Assume the file requested (file2.html) exists on the server, but is password protected. The user supplies the incorrect username/password when prompted. On your diagram you must indicate when the user is prompted for username/password. [3 marks]

Question 5 [9 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
```

Recall that the chain can be either: INPUT, OUTPUT or FORWARD. 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).

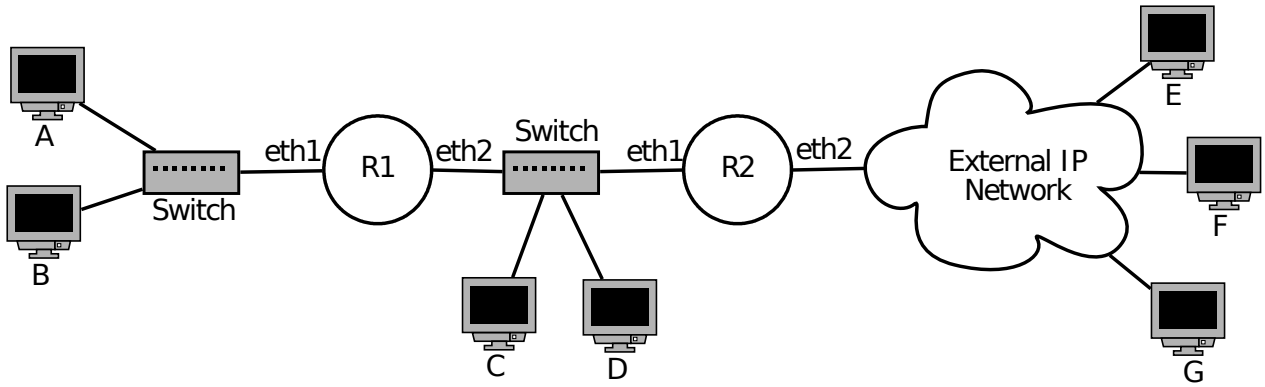

Figure 1: Firewall Network

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 DROP.

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

1. Allow all PING messages between internal and external networks. This includes allowing the firewall to send/receive PINGs. [3 marks]

2. Allow all external hosts to communicate with the web server on host B. [3 marks]

3. Allow all internal hosts, except computer C, to communicate with external Secure Shell servers. [3 marks]