00056

Sri Lanka Institute of Information Technology

B.Sc. Honours Degree in Information Technology

Specialized in Cyber Security

Final Examination
Year 2, Semester 1 (2022)

IE2012 – Systems and Network Programming(C/Python)

Duration: 2 Hours

June 2022

Instructions to Candidates:

- This paper is preceded by a 10-minutes reading period. The supervisor will indicate when answering may commence
- This paper has 4 questions.
- Answer all questions in the booklet given.
- The total mark for the paper is 100.
- This paper contains six (06) pages, including the cover page.
- Electronic devices capable of storing and retrieving text, including calculators and mobile phones are not allowed.

Question 1 [25 marks]

a) Briefly explain meaning of the following terms in related to cyber security domain [4 marks]

i. Confidentiality
ii. Integrity
iii. Authentication
iv. Authorization

b) Briefly define the usage of following basic commands in Linux with respect to man pages. You may use examples if necessary [3 marks]

i. cd .
ii. file
iii. grep

c) **"An attacker does not need to steal users' credential to login to the website as the user".**

i. Do you agree with the aforementioned statement? [1 mark]
ii. Justify your answer [4 marks]

d) Discuss the security related risk associated with HTTP GET request. You also may provide suggestions to the HTTP request to avoid the security risk issue in the GET request method [5 marks]

e) Recommend general steps to be taken when a company becomes a victim to a malware by assessing the importance of each step in the risk mitigation [8 marks]

Question 2 [25 marks]

a) Briefly explain the encapsulation process used by TCP/IP stack. [3 marks]

b) **"UDP protocol is suitable for real-time services like voice or video communication, but for Internet banking it is recommended to use TCP instead of UDP".**

i. Do you agree with the aforementioned statement? [1 mark]
ii. Justify your answer with regards to features of TCP and UDP [5 marks]

c) Describe the benefit of concurrent servers over iterative servers [4 marks]

d) Identify the STATE the socket will be moved after successful execution of following functions.

[5 marks]

i. bind ()

ii. listen ()

iii. connect ()

iv. read ()

v. accept ()

e) Answer the following questions by referring Fig. 1: strace output of iterative server and Fig. 2: strace output of client

```
[gamage@localhost SNP]$ cc -o server server.c
[gamage@localhost SNP]$ strace -e trace=network ./server
socket(PF_INET, SOCK_STREAM, IPPROTO_IP) = 3
bind(3, {sa_family=AF_INET, sin_port=htons(58005), sin_addr=inet_addr("192.168.163.130")}, 16) = 0
listen(3,2048 )                         = 0
accept(3,
```

Fig .1 : Strace output of iterative server

```
[gamage@localhost SNP]$ strace -e trace=network ./client 127.0.0.1
socket(PF_INET, SOCK_STREAM, IPPROTO_IP) = 3
connect(3, {sa_family=AF_INET, sin_port=htons(58005), sin_addr=inet_addr("127.0.0.1")}, 16) = -1
ECONNREFUSED (Connection refused)
connect error+++ exited with 1 +++
[gamage@localhost SNP]$
```

Fig .2 : Strace output of client

i. Identify the transport layer protocol used to create the socket [1 mark]

ii. Identify the bounded IP address and the port number for the server [2 mark]

iii. Does above executions return any error? [1 mark]

iv. If "Yes", identify the solution for the error generated. If "No" justify your answer [3 marks]

Question 3 [25 marks]

a) Briefly explain the purpose the OS maintain the zombie state [2 marks]

b) Define three (3) disposition methods available for signal handling in Posix signal handling environment [3 marks]

c) Compare and contrast wait () and waitpid () functions used in Zombie process handling [2 marks]

d) Followings are the outputs of successfully executed **forkserver.c** program. By referring ***"strace ./forkserver.out"*** (Fig.3) and output of ***ps –a*** command (Fig.4) given in page 4 find the answers for the given scenarios.

```
socket(PF_INET, SOCK_STREAM, IPPROTO_IP) = 3
bind(3, {sa_family=AF_INET, sin_port=htons(52001), sin_addr=inet_addr("0.0.0.0")}, 16) = 0
listen(3, 1024)                         = 0
accept(3, {sa_family=AF_INET, sin_port=htons(47563), sin_addr=inet_addr("127.0.0.1")}, [16]) = 4
clone(child_stack=0, flags=CLONE_CHILD_CLEARTID|CLONE_CHILD_SETTID|SIGCHLD, child_tidptr=0xb7534768) = 31048
close(4)                                = 0
accept(3, {sa_family=AF_INET, sin_port=htons(47564), sin_addr=inet_addr("127.0.0.1")}, [16]) = 4
clone(child_stack=0, flags=CLONE_CHILD_CLEARTID|CLONE_CHILD_SETTID|SIGCHLD, child_tidptr=0xb7534768) = 31052
close(4)                                = 0
accept(3, {sa_family=AF_INET, sin_port=htons(47565), sin_addr=inet_addr("127.0.0.1")}, [16]) = 4
clone(child_stack=0, flags=CLONE_CHILD_CLEARTID|CLONE_CHILD_SETTID|SIGCHLD, child_tidptr=0xb7534768) = 31081
close(4)                                = 0
accept(3, 0xbff29100, [16])             = ? ERESTARTSYS (To be restarted if SA_RESTART is set)
--- SIGCHLD {si_signo=SIGCHLD, si_code=CLD_EXITED, si_pid=31052, si_uid=1000, si_status=0, si_utime=0, si_stime=0} ---
accept(3,
```

Fig.3: Strace output of concurrent server

```
[gamage@localhost Reference Materials]$ ps -a
  PID TTY          TIME CMD
31033 pts/0    00:00:00 strace
31035 pts/0    00:00:00 forkserver.out
31047 pts/2    00:00:00 client.out
31048 pts/0    00:00:00 forkserver.out
31052 pts/0    00:00:00 forkserver.out <defunct>
31080 pts/4    00:00:00 client.out
31081 pts/0    00:00:00 forkserver.out
31100 pts/3    00:00:00 ps
```

Fig.4: ps –a output of concurrent server

i. Briefly explain the meaning of ***"clone"*** system call given in figure 3. [2 marks]

ii. Identify the process ID of the parent process [1 mark]

iii. Identify number of concurrent client connections initiated by the server **at the beginning**? [1 mark]

iv. Identify the **port numbers** and the **process IDs** of each client that the server is **handling at the moment** [3 marks]

v. Are there any zombie processes at the moment? If "Yes" identify the process ID of the zombie process, if "No" justify your answer [2 marks]

e) Answer following questions by referring following **tcpcliselect01.c** file

```
#include   "utils.h"        /* Header file */
void
str_cli(FILE *fp, int sockfd)
{
      int         maxfdp1;
      fd_set      rset;
      char        sendline[MAXLINE], recvline[MAXLINE];
      FD_ZERO(&rset);
      for ( ; ; )
     {
       FD_SET(fileno(fp),VAL1);
       FD_SET(VAL2 , &rset);

        maxfdp1 = max(fileno(fp), sockfd) + 1;
       // Complete the select() function
       Select();

        if (FD_ISSET(VAL3 , &rset))
        {  /* socket is readable */
          if (Readline(sockfd, recvline, MAXLINE) == 0)
            err_quit("str_cli: server terminated prematurely");
          Fputs(recvline, stdout);
         }

        if (FD_ISSET(VAL4 , &rset))
        {  /* input is readable */
          if (Fgets(sendline, MAXLINE, fp) == NULL)
            return;
          Writen(sockfd, sendline, strlen(sendline));
         }
      }

}
```

Fig.6: tcpcliselect01.c

i. Identify the missing **VAL1, VAL2, Val3** and **VAL4** [4 marks]

ii. Construct the ***select()*** function referring the program [3 marks]

iii. Discuss the importance of implementing select() function/ use of I/O multiplexing in above client program [2 marks]

Question 4 [25 marks]

a) Sketch a diagram to explain the recursive/iterative query resolution for www.lib.ruh.ac.lk. You should clearly indicate the necessary name servers. [5 marks]

b) Answer following questions by referring below python code for basic client server architecture

```
//server in python

import socket
s = socket.socket()
print('Socket Created')
s.bind(("VAL1",32007))
s.VAL2(3)
print('waiting for connections')

while True:
 c,addr=s.VAL3()
 name = c.recv(1024).decode()
 print("Connected with " , addr, name)
 c.send(bytes('Welcome to SNP','utf-8'))
 c.close()
```

```
//client in python

import socket

c = socket.VAL4()

c.VAL5(("127.0.0.1",32007))

name = input("Enter name:")
c.VAL6(bytes(name,'utf-8'))

print(c.recv(1024).decode())
```

i. Provide the values of **VAL1, VAL2, VAL3, VAL4, VAL5** and **VAL6** [6 marks]

ii. Define default values used by ***socket ()*** function if user not define any parameters [2 marks]

iii. Identify the output that will be printed in the server terminal after successful execution of server and client programs

Hint: You may use your name for the "name" variable [4 marks]

c) Develop a bash script: the script should use a function named "**welcomeStudent**" to execute the below tasks [4 marks]

- Take a student name as a command line variable
- If the above variable is null script should stop execution (exit)
- Write a welcome message using the above variable ***(Ex: Welcome <name>)*** to a file name "**welcomeMe.txt**"

  (Hint: Content does not need to be appended to the file)
- Move the **"welcomeMe.txt"** file to **user's home directory.** (User's name should not be hard coded)

d) Recommend the steps to be followed if above script need to be executed periodically

(Hint: scheduled to be run in every 3 days at 8.00 am) [4 marks]