PES UNIVERSITY	PES University, Bengaluru (Established under Karnataka Act No. 16 of 2013)
December 2020: End Semester Assessment B.TECH. VII Semester Elective CSE UE17CS421: INFORMATION SECURITY	
Time: 180 Mins	Answer All Questions — Max Marks: 100

Questions		Marks
Q 1A	Based on the security principles discussed in lecture identify the principle(s) relevant to each of the following scenarios:	
	1. New cars often come with a valet key. This key is intended to be used by valet drivers who park your car for you. The key opens the door and turns on the ignition, but it does not open the trunk or the glove compartment.	1
	2. Many home owners leave a house key under the floor mat in front of their door.	1
	3. Shamir's secret sharing scheme allows us to split a "secret" between multiple people, so that all of them have to collaborate in order to recover the secret.	1
	4. Banks often make you answer your security questions over the phone. Answers to these questions are "low entropy", meaning that they are easy to guess. Some security conscious people instead use a random password as the answer to the security question. Ex: Q: "What is your dog's maiden name?". A: "60ba6b1c881c6b87" However, attackers can sometimes convince the phone representative by claiming "I just put in some nonsense for that question".	2
Q 1B	The `chown` command automatically disables the Set-UID bit, when it changes the owner of a Set-UID program. Please explain why it does that.	4

Q 1C	When a program takes an input from users, we can redirect the input device, so the program can take the input from a file. For example, we can use `prog < myfile` to provide the data from myfile as input to the prog program. Now, if prog is a root- owned Set-UID program, can we use the following method to get this privileged program to read from the /etc/shadow file? `$ prog < /etc/shadow`	5

Q 1D	The following are two different ways to printout environment variables. Please describe their differences:
	
	`$ /usr/bin/env`
	`$ /usr/bin/strings /proc/$$/environ`
		6

Q 2A	In a Linux system, a privileged Set-UID program needs to find out which directory it is currently in. As a Security Engineer, which approach would you use? Explain. One is to use the PWD environment variable, which contains the full path of the current directory. Another approach is to use the `getcwd()` which is a system call in Linux.	5

Q 2B	Instead of putting an extra shell command after a function definition, we put it at the beginning (see below).
	
	`$ export foo='echo world; () { echo hello;}'`
	`$ bash`
	We then run Bash, which is vulnerable to the Shellshock attack. Will the shell command `echo world` be executed?
		4

Q 2C	We run "nc -l 7070" on Machine 1 (IP address is 10.0.2.6), and then type the following command on Machine 2. `$ /bin/cat < /dev/tcp/10.0.2.6/7070 >&0` Describe what happens?	3

Q 2D	Consider the following program:
	
	`#include <stdio.h>`
	`#include <stdlib.h>`
	`#include <unistd.h>`
	
	`extern char **environ;`
	
	`int main()`
	`{`
	`  char *args[] =`
	`  {`
	`  "/bin/sh", "-c",`
	`  "/bin/ls", NULL`
	`  };`
	`  pid_t pid = fork();`
	
	`  if(pid == 0) { /* child */`
	`  printf("child\n");`
	`  execve(args[0], &args[0], NULL);`
	`  }`
	`  else if(pid > 0) {`
	`  /* parent */`
	`  printf("parent\n");`
	`  }`
	`  return 0;`
	`}`
	
	The program is executed as the following.
	
	`$ gcc prog.c -o prog`
	`$ export foo='() { echo hello; }; echo world;'`
	`$ ./prog`
	
	Explain what the output of the program will be and why.
		8

Q 3A	Your Manager says the below program does NOT have Buffer overflow. Do you agree? Justify your position.	5

	`int bof(char *str, int size)`
	`{`
	`  char *buffer = (char *) malloc(size);`
	`  strcpy(buffer, str);`
	`return 1;`
	`}`	

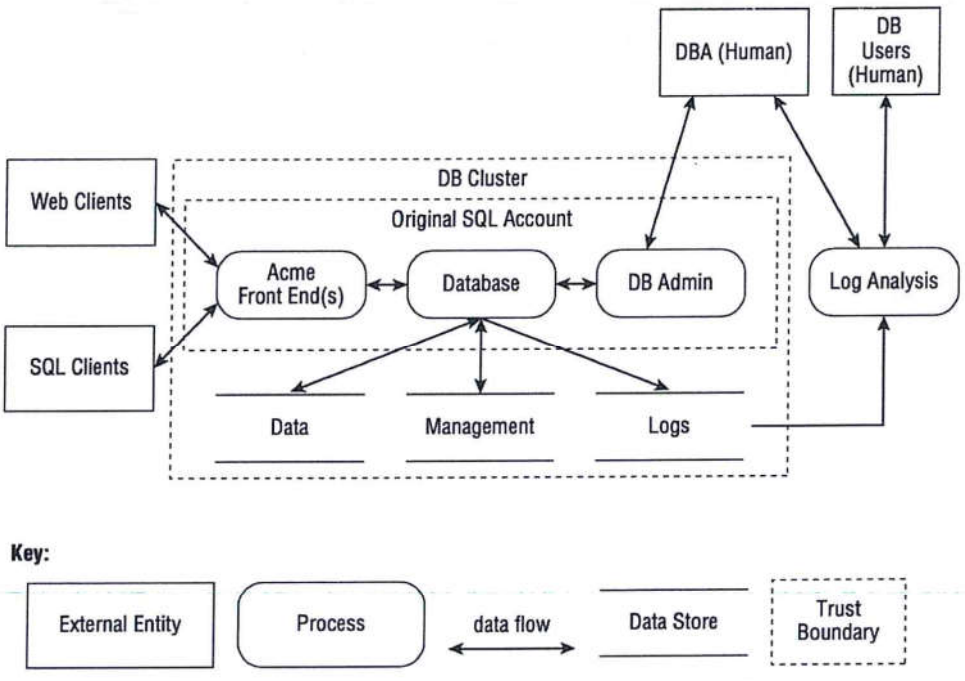
Q 3B	Students were working on the Buffer Overflow attacks. One student obtained the below output. Can you explain why the student got shell access in some cases and not in others?
	
	`buffer address : 0xbffff180`
	`case 1 : long retAddr = 0xbffff250 -> Able to get shell access`
	`case 2 : long retAddr = 0xbffff280 -> Able to get shell access`
	`case 3 : long retAddr = 0xbffff300 -> Cannot get shell access`
	`case 4 : long retAddr = 0xbffff310 -> Able to get shell access`
	`case 5 : long retAddr = 0xbffff400 -> Cannot get shell access`
		5

Q 3c	Can we use the StackGuard idea to protected against format-string attacks? Explain	5

Q 3D	A very general depiction of virus code V is shown in below.
	
	In this case, the virus code, V, is prepended to infected programs, and it is assumed that the entry point to the program, when invoked, is the first line of the program. Determine if there is any flaw in this code. Justify.
	
	`program V :=`
	`{goto main;`
	`1234567;`
	`subroutine infect-executable :=`
	`{loop:`
	`file := get-random-executable-file;`
	`if (first-line-of-file = 1234567)`
	`then goto loop`
	`else prepend V to file; }`
	`subroutine do-damage :`
	`{whatever damage is to be done}`
	`subroutine trigger-pulled :`
	`{return true if some condition`
	`holds}`
		5

```
main:          main-program :=

                    {infect-executable;
                     if trigger-pulled then do-
damage;
                     goto next;}
next:
}
```

Q 4A	To defeat XSS attacks, a developer decides to implement filtering on the browser side. Basically, the developer plans to add JavaScript code on each page, so before data are sent to the server, it filters out any JavaScript code contained inside the data. Let's assume that the filtering logic is perfect. Can this approach prevent XSS attacks?	5
Q 4B	The diagram below shows the Data flow for ACME SQL database.  Can you perform a Threat Modelling using STRIDE?	6
Q 4C	A e-commerce website has many product categories; When the user selects a category, the application carries out an SQL query like the following:	3

	`SELECT * FROM products WHERE category = 'Gifts' AND released = 1` Which SQL attack statement would you use to perform an SQL injection attack that causes the application to display details of all products in any category, both released and unreleased.	
Q 4D	The code below shows a SQL injection attack that runs a DROP command to remove the users table entirely, in order to corrupt the database. `statement.executeQuery("SELECT * FROM users WHERE email='billy@gmail.com'; DROP TABLE users;--' AND encrypted_password='Z$DSA92H0'");` Explain and rewrite the query to mitigate the attack.	6

Q 5A	Consider the C program below.
	
	After your code review what suggestions would you give the developer?
	
	`1 typedef enum { red, green, blue } Color;`
	`2`
	`3 char* getColorString(Color c) {`
	`4  char* ret = NULL;`
	`5  switch (c) {`
	`6  case red:`
	`7  printf("red");`
	`8  }`
	`9  return ret;`
	`10 }`
		6

Q 5B	How are the addresses decided for the following variables a and i, i.e., during the run- time, how does the program know the address of these two variables?
	
	`void foo(int a)`
	`{`
	`int x; }`
		2

Q 5C	A team member has written the below code in C;. The code prints a message to a specified file descriptor.
	
	`void printMsg(FILE* file, char* msg) {`
	`  fprintf(file, msg);`
	`}`
	
	After performing static analysis, the team manager notes that the code does not perform any error checking!
	
	Please rewrite the code to include the three error checks that the team member should add.
		9

5 QD	1. _____deals with the protection of an individual's information which is implemented while using the Internet on any computer or personal device. a) Digital agony b) Digital privacy c) Digital secrecy d) Digital protection 2. Which of the following is not an appropriate solution for preserving privacy? a) Use privacy-focussed SE b) Close all logical ports c) Do not use malicious sites and torrent sites d) Use VPN	1 1

	3. The _____ protects your privacy by bouncing your connection and links around a distributed network over the globe run by volunteers. It gives three layers of anonymity. a) Cookie removers b) Private Search Engines c) Tor browser d) VPNs	1