Question 1

Not yet graded / 2 pts

Write the Google search syntax for the following:

- The page title contains "index of"
- The page body contains the keyword "mp4"
- The page body is NOT in the "labtabs.edu.au/ domain

Question 2

Not yet graded / 1 pts

Briefly describe how you would architect and embed the "defence in depth" engineering principle in order to try to mitigate the risk posed by ransomware delivered by email attachment?

Question 3

0 / 1 pts

Ransomware causes impact on which attribute(s) of information security?

- Confidentiality
- Integrity
- Availability
- Non-Repudiation

Question 4

0 / 1 pts

What kind of control is pentestration testing in the context of security management?

- Corrective
- Administrative
- Preventive
- Detective

Question 5

Not yet graded / 2 pts

Write a proof-of-concept payload to exploit the XSS vulnerability in the following PHP code, so that the browser will show an alert() popup. Assume there is a cookie that stores data with name 'color'.

```
<?php
$color = $_COOKIE['color'];
$msg = "<div color='" . $color . "'>Welcome to CS4153</div>";
echo $msg;
?>
```

Question 6

Not yet graded / 4 pts

Suppose a web application has two tables: (1) the first one contains id, firstname, lastname and (2) the second one contains id, password (containing SHA1 hash of the user password).

The following PHP searches for users in the Users table and displays firstname and lastname:

```
<?php

// get input
$x = $_POST['x' ];

// search database
$query = "SELECT id, firstname, lastname FROM users WHERE lastname LIKE '%' . $x . "%'";
$result = mysqli_query($connection, $query );

// get results -- display all hits
while ($row = mysqli_fetch_assoc( $result ) ) {
  $first = $row["firstname"];
  $last = $row["lastname"];

  ...

// print results
$msg .= "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
}

echo $msg;
?>
```

What payload can you inject into the "x" parameter to get the program to show the list of ALL users in the Users table followed by ALL the passwords from the Password table?

Question 7

Not yet graded / 2 pts

Name two techniques that can be used to force the victim to browse to a malicious website when it tries to browse facebook.com.

Your answer:

Question 8

Not yet graded / 2 pts

Name two important skills/attributes that are important for becoming an effective cyber security specialist.

Your answer:

Question 9

Not yet graded / 1 pts

Please briefly describe what black hat, white hat, and grey hat hackers are.

Question 10

Not yet graded / 1 pts

Refer to the program below. Is it possible to change the value of 'grade' by inputting numbers of 'A's into the memory, which will cause a buffer overflow and overwrite the 'grade' as 'A'? Briefly explain why.

```
#include <stdio.h>
#include <stdio.h>

int main(int argc, char** argv)
{
  char buff[20];
  char grade[2 ] = "F";
  printf("Enter a your name? ");
  gets(buff);
  printf("Hello %s! Your grade is %s.\n", buff, grade);
  return 0;
}
```

Question 11

Not yet graded / 4 pts

Refer to the C code below. Suppose this is compiled with the -fstack-protector and -z noexecstack options. Can you craft an input to force the program to print "Hack"? Explain.

Assume you are not allowed to "patch" the compiled binary.

```
#include <stdio.h>
#include <stdio.h>

int main(int argc, char** argv)
{
  int check = 0xDE;
  char buff[16];
  char* ptr = buff;
  if(check == 0xDE)
    printf("Pass");
  else if(check == 0xAD)
    printf("Hack");
  return 0;
}
```

Question 12

0 / 1 pts

True of False. An application that is vulnerable to GET type CSRF can be exploited simply by tricking the victim to load an image on the browser.

- True
- False

Question 13

0 / 1 pts

True or False? It is legal for ethical hackers trying to defend an organisation's IT systems to launch a denial of service (DoS) attack against a malicious attacker to prevent intrusions.

- True
- False

Question 14

0 / 1 pts

The techniques for hiding data inside a "cover" image using the pixel bits in a way that will not alter the original image noticeable is known as ___ steganography.

Question 15

0 / 1 pts

RISK MATRIX					
CONSEQUENCE / LIKELIHOOD	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Extreme
a - Almost certain (frequent)	M	M	H	E	E
b - Likely (probable)	L	M	H	H	E
c - Possible (occasional)	L	M	M	H	H
d - Unlikely (uncommon)	L	L	M	M	H
e - Rare (remote)	L	L	L	L	M

Suppose the consequence (impact) of a successful credential theft via phishing is deemed "Major" for an organisation. If the organisation's risk appetite is Medium (i.e., all risks must be reduced to at least Medium), countermeasures must be implemented to reduce the likelihood to ___.

Question 16

Not yet graded / 2 pts

Name two security engineering principles (or rules of thumb)

Question 17

Not yet graded / 1 pts

Calculate the ALE (annualised loss expectancy) in the following scenario describing the risk of damages to the data centre due to flooding. Answer in 100s of dollars (e.g., $100K -> $100).

- Data centre is worth $10 million dollars
- Flooding takes place every 100 years
- In the event of a flood, 75% of data centre is damaged beyond repair

Question 18

Not yet graded / 1 pts

How is SIEM different from IDS?

Your answer:

Question 19

Not yet graded / 2 pts

Which of the following uses the RC4 cipher?

A. WEP
B. WPA2
C. WPA2-PSK

Your answer:

Question 20

0 / 1 pts

A Man-in-the-Middle (MitM) attack is a type of cyber attack where an attacker inserts themselves between two communicating parties, the sender and the receiver, without their knowledge. In a MITM, what does an attacker do? Choose all that apply.

- Intercepting the communication
- Eavesdropping
- Impersonating the parties
- Modifying the communication

Question 21

Not yet graded / 2 pts

What is a deceception? What are its primary use cases?