

Question 1	Not yet graded / 2 pts
<p>Write the Google search syntax for the following:</p> <ul style="list-style-type: none"> • The page title contains "index of" • The page body contains the keyword "mp3" • The page body is NOT in the "sabalado.edu.au/" domain 	

Question 2	Not yet graded / 1 pts
<p>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 attachments?</p>	

Question 3 0 / 1 pts

For software classes, impact on which attribute(s) of information security?

- ☐ Confidentiality
- ☐ Integrity
- ☒ Availability
- ☐ Non-Repudiation

Question 4

0 / 1 pts

What kind of control is penetration 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().
pnpnp. Assume there is a cookie that stores data with name 'color'.

```
<div>  
    $color = $_COOKIE["color"];  
    $html = "<div color='\" . $color . "\">";  
    echo $html;  
</div>
```

[illegible]

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
<p>Name two important skills/attributes that are important for becoming an effective cyber security specialist.</p>	
<p>Your answer:</p>	

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 injecting numbers of 'A's into the memory, which will cause a buffer overflow and overwrite the 'grade' as 'A'? Briefly explain why.

```
#include <iostream.h>
#include <string.h>

int main(int argc, char** argv)
{
    char buf[1024];
    char str[10];
    printf("What is your name? ");
    gets(buf);
    printf("%s but your grade is %s\n", buf, grade);
    return 0;
}
```

Question 11

Not yet graded / 4 pts

Refer to the C code below. Suppose this is compiled with the `-fsanitize=address` and `-fno-sanitize-recover` options. Can you craft an input to leave the program in state `0x00000000` again?

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

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

int main(int argc, char** argv)
{
    int check = 0;
    char buffer[10];
    getBuffer();
    printf("0x%08x\n",
        (int) getChar() % 0x10);
    exit(0);
}
```

Question 12 0 / 1 pts

True or 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 organization's IT systems to launch a denial of service (DoS) attack against a malicious attacker to prevent intrusion.

☐ 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 noticeably is known as ____ steganography.

Question 15		Risk Matrix				
LIKELIHOOD	CONSEQUENCE	RISK MATRIX				
		1	2	3	4	5
		Insignificant	Minor	Moderate	Major	Extreme
1	A - Almost certain (Frequent)	M	M	M	H	E
2	B - Likely (Frequent)	L	M	M	H	E
3	C - Possible (Intermittent)	L	M	M	H	E
4	D - Unlikely (Uncommon)	L	L	M	H	E
5	E - Rare (Unusual)	L	L	M	H	E

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 ALZ (unrealised 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., 1000K => 1000K.

- Data centre is worth \$30 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 pt

How is SISM different from ISM?

Your answer:

Question 19 Not yet graded / 2 pts

Which of the following uses the RC4 cipher?

- A. WEP
- B. WPA3
- C. WPA2-PSK

Your answer:

Question 20

0 of 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 MTM, 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 descompline? What are its primary use cases?