```
Not yet graded / 2 pts
Question 1
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 "adelaide.edu.au" domain

                                                                                                                 Not yet graded / 1 pts
Question 2
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?
                                                                                                                             0 / 1 pts
Question 3
Ransomware causes impact on which attribute(s) of information security?
    Confidentiality
    Integrity
    Availability
    Non-Repudiation
                                                                                                                             0 / 1 pts
Question 4
What kind of control is penetration testing in the context of security management?
    Corrective
    Administrative
    Preventive
    Detective
                                                                                                                 Not yet graded / 2 pts
Question 5
Write a proof-of-concept payload to exploit the XSS vulnerability in the following PHP code, so that the browser will show an alert(1)
popup. Assume there is a cookie that stores data with name 'color'.
 $color = $_COOKIE['color'];
$html = "<div color='" . $color . "'>Welcome to CSF</div>";
 echo $html;
                                                                                                                 Not yet graded / 4 pts
Question 6
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
 $s = $_REQUEST[ 's' ];
 // Search database
 $query = "SELECT id, firstname, lastname FROM Users WHERE lastname LIKE '%" . $s . "';"
 $result = mysqli_query($connection, $query )
 // Get results -- display all hits
 while ($row = mysqli_fetch_assoc( $result ) ) {
   $first = $row["firstname"];
   $last = $row["lastname"];
 // Print results
 $html .= "ID: {$id}<br />First name: {$first}<br />Surname: {$last}";
 echo $html;
 ?>
What payload can you inject into the "s" 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?
                                                                                                                 Not yet graded / 2 pts
Question 7
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:
                                                                                                                 Not yet graded / 2 pts
Question 8
Name two important skills/attributes that are important for becoming an effective cyber security specialist.
Your answer:
                                                                                                                 Not yet graded / 1 pts
Question 9
Please briefly describe what black hat, white hat, and grey hat hackers are.
                                                                                                                 Not yet graded / 1 pts
Question 10
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 <stdlib.h>
 #include <stdio.h>
 int main(int argc, char** argv)
    char buff[10];
    char grade[] = "F"
     printf("What is your name? ");
     gets(buff);
     printf("Hello %s! Your grade is:%s.\n", buff, grade);
     return 0;
                                                                                                                 Not yet graded / 4 pts
Question 11
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 "Yes!"? Explain.
Assume you are not allowed to "patch" the compiled binary.
 #include <stdio.h>
 #include <stdlib.h>
 int main(int argc, charr** argv)
     int check = 2021;
    char buff[12];
     gets(buff);
     if(check == 2019)
         printf("Yes!");
     else
         printf("No");
     return 0;
                                                                                                                             0 / 1 pts
Question 12
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.
    O True
    False
                                                                                                                             0 / 1 pts
Question 13
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.
    O True
    False
                                                                                                                             0 / 1 pts
Question 14
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.
                                                                                                                             0 / 1 pts
Question 15
                                                            RISK MATRIX
                    CONSEQUENCE
 LIKELIHOOD
                                        Insignificant
                                                                                Moderate
                                                              Minor
                                                                                                    Major
                                                                                                                      Extreme
 a - Almost certain (frequent)
                                             M
                                                                M
                                                                                   н
 b - Likely (probable)
                                                                M
                                                                                   н
 c - Possible (occasional)
                                                                M
                                                                                  M
 d - Unlikely (uncommon)
                                                                                  M
                                                                                                      M
 e - Rare (remote)
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 ___.
                                                                                                                 Not yet graded / 2 pts
Question 16
Name two security engineering principles (or rules of thumb)
                                                                                                                 Not yet graded / 1 pts
Question 17
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

                                                                                                                 Not yet graded / 1 pts
Question 18
How is SIEM different from IDS?
Your answer:
```

Not yet graded / 2 pts

0 / 1 pts

Not yet graded / 2 pts

Question 19

A. WEP

B. WPA3

Your answer:

Question 20

C. WPA2-PSK

Which of the following uses the RC4 cipher?

Intercepting the communication

Impersonating the parties

Modifying the communication

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

Eavesdropping

Question 21

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.