Family Name:. . . . . **First Name:**. . . . .

Student ID:. . . . . **Signature**. . . . .

CYBR 171: TRIMESTER 1 – TEST 2

June 15, 2022

Instructions

- Time allowed: **120 minutes**
- **CLOSED BOOK**
- **Permitted materials**
  - Only silent non-programmable calculators or silent programmable calculators with their memories cleared are permitted in this test.
  - Printed English to foreign language dictionaries are permitted.
  - No other material is permitted.
- Attempt **ALL** questions in this booklet.
- This test contributes 25% of your final grade.
- Section A on pages 3 to 7 has TWENTY-SEVEN multi-choice questions.
- Section B on pages 9 and 10 has EIGHT multi-choice questions.
- Choose your answer for each question in Sections A and B, and mark it on the multi-choice answer sheet provided, **NOT** in this question booklet. Any answers for Sections A or B in the question booklet **WILL NOT BE MARKED**.
- Read the instructions given on the answer sheet on how to mark your answers.
- **Hand in the multi-choice answer sheet.**
- Section C on pages 11 and 12 has FOUR written short answer questions.
- Write answers to Section C in the spaces provided in the test booklet.
- **Hand in the test booklet.**

Questions	**Marks**	
1. Section A - CONCEPTS	[27]	□
2. Section B - APPLYING CONCEPTS	[16]	□
3. Section C - SHORT ANSWERS	[12]	□
	TOTAL:	□

This page intentionally left blank.

SECTION A CONCEPTS [27 marks]

Each question in this section is worth ONE mark.

Question 1. What is the MOST secure default firewall policy?

A. All computers on the local area network can access any service on the Internet.

B. No computers on the local area network can access the Internet.

C. Some computers on the local area network can access any service on the Internet.

D. Some computers on the local area network can access specific services on the Internet.

Question 2. Your Intrusion Detection System (IDS) reports an attack but on investigation you discover that this was an error. What type of error is this?

A. False negative.

B. False positive.

C. True negative.

D. True positive.

Question 3. What is a vulnerability in a web application that allows a hacker to force another user to execute malicious code?

A. Cross-site scripting (XSS).

B. Path traversal.

C. SQL injection.

D. XML injection.

Question 4. Which of the following is a WEAKNESS of misuse detection as opposed to anomaly detection?

A. Does not require regular updates.

B. Less likely to raise false alarms.

C. Misses new types of attack.

D. Performance increases as add more rules.

Question 5. Which of the following techniques can be used to stop a cross-site request forgery (CSRF) attack on a web application?

A. Re-authenticate every request.

B. Sanitize user controlled data.

C. Set secure flag on cookie.

D. Use access controls.

Question 6. Which of the following is TRUE for the "steal the cookie" attack?

A. Allows an attacker to impersonate the user.

B. Can ONLY be prevented by setting the secure flag on a cookie.

C. Exposes the user's password to the attacker.

D. Prevention only requires the login page to be protected by HTTPS.

Question 7. Consider HTML forms, _____ sends the values as query string parameters as part of the URL whereas _____ sends them as hidden within the HTTP request body.
Choose the pair below that would best complete the sentence above.

A. GET, GET.

B. GET, POST.

C. POST, GET.

D. POST, POST.

Question 8. A _____ XSS attack requires the web site to have some way to return a script provided by one user to another at a later point in time.
A _____ XSS attack may return a script immediately to a user via a error message.
Which of the following pairs correctly complete the two sentences above.

A. Reflected, Reflected.

B. Reflected, Stored.

C. Stored, Reflected.

D. Stored, Stored.

Question 9. Which of these statements is TRUE about the following firewall rule, considering 192.168.0.50 is the IP address of a machine on the internal network?

direction	src	dst	protocol	dest port	action
in	*	192.168.0.50	*	*	allow

A. All communications from a specific machine on the internal network to any external machine is allowed.

B. All inbound traffic to all machines on the internal network is allowed.

C. Inbound traffic to a specific machine on the internal network is allowed.

D. Only inbound HTTP traffic to a specific machine on the internal network is allowed.

Question 10. Phishing relies primarily on the following:

A. Benefit in exchange for information.

B. Brute forcing a password.

C. False sense of urgency.

D. Tailgating.

Question 11. Which of the following descriptions most closely describes a VPN?

A. Guaranteed anonymity for users.

B. High speed connection.

C. Reliable connection to a corporate network.

D. Private connection across an untrusted network.

Question 12. Which of the following social engineering attacks is considered to be a form of a 419 scam?

A. Baiting.

B. Email compromise and fake invoice scam.

C. Spanish prisoner.

D. Tailgating.

Question 13. Which of the following psychological experiments investigated people's willingness to obey others even if asked to do immoral things?

A. Asch's experiment.

B. Jones & Harris' experiment.

C. Milgram's experiment.

D. Zimbardo's prisoner experiment.

Question 14. Which of the following psychological experiments investigated whether people would rather conform and deny the evidence of their senses?

A. Asch's experiment.

B. Jones & Harris' experiment.

C. Milgram's experiment.

D. Zimbardo's prisoner experiment.

Question 15. What is considered to be the weakest link in any security system?

A. Cryptography.

B. Legal powers.

C. Passwords.

D. People.

Question 16. What human emotion does Pre-texting exploit?

A. Anxiety.

B. Fear.

C. Sadness.

D. Trust.

Question 17. Which of the following types of security are concerned with attacks such as the theft of a USB containing sensitive information?

A. Application.

B. Network.

C. Physical.

D. Web application.

Question 18. The correct ordering of the steps involved in a social engineering attack is:

A. Define your goal, build trust, exploit the relationship, seek information and use the information gathered for malicious purposes.

B. Define your goal, build trust, seek information, exploit the relationship and use the information gathered for malicious purposes.

C. Define your goal, build trust, seek information, use the information gathered for malicious purposes and exploit the relationship.

D. Define your goal, seek information, build trust, exploit the relationship and use the information gathered for malicious purposes.

Question 19. Which one of the following categories of protection component would Ruapekapeka's location inland from the coast BEST fit?

A. Deter.

B. Alarm.

C. Detect.

D. Delay.

Question 20. Which one of the following categories of protection component would Ruapekapeka's position on the hill allowing easy visibility of the British encampment BEST fit?

A. Alarm.

B. Delay.

C. Detect.

D. Respond.

Question 21. What is the BEST description of the principle of defence-in-depth?

A. Minimise privilege required by users.

B. Multiple protection components.

C. Strong encryption.

D. Strong protection components.

Question 22. Which of the following terms describe the set of instructions and actions to be performed at every step in the incident response (IR) process?

A. Analysis steps.

B. Playbook.

C. Response plan.

D. Recovery manual.

Question 23. What is the definition of *real* evidence as discussed in the lectures?

A. Any evidence given by a first party.

B. Any evidence such as an inanimate object.

C. Any hearsay evidence.

D. The best or "first hand" evidence.

Question 24. What does the acronym CSIRT stand for?

A. Computer Security Incident Reaction Team.

B. Computer Security Incident Response Team.

C. Cyber Security Incident Reaction Team.

D. Cyber Security Incident Response Team.

Question 25. Which of the following correctly lists the <u>first four</u> steps of the cyber kill chain?

A. Delivery, Weaponization, Reconnaissance, Exploitation.

B. Exploitation, Reconnaissance, Weaponization, Delivery.

C. Reconnaissance, Weaponization, Delivery, Exploitation.

D. Weaponization, Reconnaissance, Delivery, Exploitation.

Question 26. Which statement regarding tabletop exercises is <u>FALSE</u>?

A. Allows you to test the plan and playbooks.

B. Identifies whom to blame.

C. Identify gaps in the plans or playbooks.

D. Led by a facilitator.

Question 27. Which one of the following is the correct definition of Locard's exchange principle as discussed in the lectures?

A. A trace left by an event will be visible on the objects involved.

B. When an event happens, it leaves a trace.

C. When an event affects an object, it will leave a trace of it's occurrence.

D. When two objects come into contact, they leave a trace on each other.

This page intentionally left blank.

SECTION B APPLYING CONCEPTS [16 marks]

Each question in this section is worth TWO marks.

Question 28. What is the main reason for the discussion of physical security in a course on cybersecurity?

A. Attackers might damage your property through vandalism.
B. Attackers might dumpster dive to steal commercial secrets.
C. Attackers might target your physical cash for theft.
D. Attackers might use physical access to defeat any of your security technologies.

Question 29. Which one of the following statements about a protection system is FALSE?

A. Both physical and software components may be included.
B. Ideally has multiple layers of defence.
C. Usually has a goal.
D. Will always protect all assets.

Question 30. A long-anticipated PC game is about to be released. An attacker makes available a pre-release copy of the game available via a file sharing service via BitTorrent. The game is actually a trojan that will allow the attacker to steal banking information.
What type of attack would you classify this as?

A. Baiting.
B. Phishing.
C. Pre-texting.
D. Quid Pro Quo.

Question 31. A scammer stops people on the street and invites them to take part in a prize draw for the Mother's day. They can participate as long as they provide their full name, date of birth, email address and mother's maiden name.
Which of the following is the best description of this scam?

A. Baiting.
B. Phishing.
C. Pre-texting.
D. Quid Pro Quo.

Question 32. Tech support scams are quite common in New Zealand. These scammers use familiar brand names such as Microsoft, Spark, Vodafone and Chorus. They may call on the phone and will often attempt to get "remote access" to your device. Remote access is when someone can access a computer or a network from another location.
What type of attack would you classify this as?

A. Baiting.
B. Phishing.
C. Pre-texting.
D. Quid Pro Quo.

Question 33. Consider a small coffee shop in an outdoor shopping area. Several nearby shops have been broken into overnight to steal money kept overnight. The attackers broke the glass window at the front of these shops to enter.
Which is the <u>CHEAPEST</u> option to deter attackers?

A. Cover all the windows with metal shutters.

B. Employ a security guard.

C. Install a safe.

D. Put up a sign saying "no money is kept overnight".

Question 34. Imagine a building with a front door that requires a swipe card to open. Attackers are gaining unauthorised access to the building by tailgating.
How would you <u>BEST</u> prevent this happening?

A. Add an employee photo to the swipe card.

B. Place better lighting over the door to remove shadows where attackers might hide.

C. Replace swipe cards with physical keys.

D. Replace the door with a swipe card controlled turnstile that only allows one person at a time to enter.

Question 35. Assume that a target has previously been told by their IT department not to install programs sent as attachments. How would you design an attack based upon the findings from Solomon's Asch's 1951 experiment?

A. Identify the target's bank. Send an email claiming to be from the bank that encourages the target to install a secure messaging program attached to the email in order to complete a pending transaction. The secure messaging program is actually ransomware.

B. Identify the target's boss. Send an email from the boss that orders the target to install a secure messaging program attached to the email. The secure messaging program is actually ransomware.

C. Identify the target's friends. Send multiple emails claiming to be from their friends and encourages the target to install a secure messaging program attached to the email by saying that the attached program. The secure messaging program is actually ransomware.

D. Identify well-known security professional that the target follows on LinkedIn. Send an email claiming to be from the security professional that encourages the target to install a secure messaging program attached to the email by appealing to the target's fear of being spied upon. The secure messaging program is actually ransomware.

SECTION C SHORT ANSWERS [12 marks]

Each question in this section is worth THREE marks.

Question 36. Explain why it is extremely important to properly handle digital evidence such as hard disk drives, and what could be the consequences if the data collection process did not prevent data manipulation. [3 marks]

Question 37. Briefly explain why when performing *certain* critical tasks on some websites you are asked to reauthenticate yourself. [3 marks]

Question 38. Explain why it is important to have multiple mechanisms in each layer of the security system. [3 marks]

Question 39. List FOUR differences between legal issues (Law) and ethical issues (Ethics)? [3 marks]

* * * * * * * * * * * * * * *

Student ID: . . . .

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.