TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

EXAMINATIONS – 2019

TRIMESTER 1

CYBR 171

CYBERSECURITY FUNDAMENTALS

Time Allowed: TWO HOURS ******** WITH SOLUTIONS **********

CLOSED BOOK

Permitted materials: Only silent non-programmable calculators or silent programmable calculators with their memories cleared are permitted in this examination.

Printed foreign to English language dictionaries are permitted.

No other material is permitted.

Instructions: There are TWO sections.

Attempt ALL questions in each section.

Section A on pages 2 to 12 has 50 multi-choice questions. Each question is worth a $\frac{1}{2}$ mark. The total for Section A is 25 marks.

Choose the best answer for each question in Section A and mark it on the multi-choice answer sheet provided, not in this question booklet.

The answer sheet has space for 60 questions.

Only fill in questions 1 to 50.

Hand in the multi-choice answer sheet.

Section B on pages 13 to 15 has written answer questions. Each question is worth FIVE marks. The total for Section B is 15 marks.

Write answers to Section B in the spaces provided in the examination booklet.

Hand in the examination booklet.

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.

SECTION A [25 marks]

- *Each question is worth a $\frac{1}{2}$ mark.*
- *Select the best answer and mark the appropriate letter on the multi-choice answer sheet provided.*
- *Read the instructions given on the answer sheet on how to mark your answers.*
- *Your answers must be on the multi-choice answer sheet, not on this question booklet.*

Fundamental Concepts

1. Which security property is breached by an unauthorized disclosure of information?
    A. Confidentiality.
    B. Authenticity.
    C. Availability.
    D. Integrity.

    Confidentiality

2. Which of the following assures that a system performs its intended function in an unimpaired manner?
    A. Availability.
    B. Confidentiality.
    C. Data Integrity.
    D. System Integrity.

    System Integrity

3. Evaluate the truth of the statement *checking the integrity of data relies upon being able to authenticate who is requiring access?*:
    A. TRUE because we need to be able to control who is allowed to modify it.
    B. TRUE because we need to be able to track who has modified it.
    C. FALSE because we only need to know whether its has been modified or not.
    D. FALSE because it will not allow us to identify changes by unknown users.

    C - FALSE

4. The term *leaky* relates to a loss of:
    A. Availability.
    B. Confidentiality.
    C. Data Integrity.
    D. System Integrity.

    Loss confidentiality

5. An *active* attack is one where the attacker.
    A. Alters system resources.
    B. Launches the attack from inside the security perimeter.
    C. Launches the attack from outside the security perimeter.
    D. Makes use of information from the system that does not affect system resources.

    Alters system resources

6. A countermeasure is:
    A. A way to mitigate a risk.
    B. A way to recover from an attack.
    C. Only mitigates threats.
    D. Only mitigates vulnerabilities.

    only mitigates threats that is anything that could lead to an attack

7. What risks should you consider when doing a risk assessment?
    A. Those with matching threats.
    B. Those with matching vulnerabilities.
    C. Those where there is a threat with a matching vulnerability.
    D. Those where there has been an attack.

    there is a matching threat with matching vulnerability

    Cryptography

8. Which of the following is a symmetric cryptography algorithm?
    A. Diffie-Hellman.
    B. SHA-2.
    C. Triple DES.
    D. RSA.

    Triple DES

9. Which of the following modes of operations will allow you to detect if the blocks in an encrypted message are re-arranged?
    A. AES.
    B. CBC.
    C. ECB.
    D. Blowfish.

    CBC

10. Which of the following cryptographic mechanisms allow you to determine that data originated with an author?

    A. Asymmetric cryptography.
    B. Digital certificate.
    C. Digital signature.
    D. Hash.

    Digital certificate

11. Calculate how many secret keys will be required for SIX parties who want to set up secure two-way communication with each other using *symmetric* cryptography.

    A. 1.
    B. 6.
    C. 15.
    D. 24.

    15 - (n-1) * n divide by 2 because symmetric

12. Calculate how many secret keys will be required for SIX parties who want to set up secure two-way communication with each other using *asymmetric* cryptography.

    A. 1.
    B. 6.
    C. 15.
    D. 24.

    only need a public key and private key

13. If two values map to the same hash value, what is it called?

    A. Birthday Problem.
    B. Collision.
    C. Diffusion.
    D. Replication.

    Collision

14. What security service determines which resources a user can access along with the operations that a user can perform?

    A. Authentication.
    B. Authorization.
    C. Biometric.
    D. Token.

    Authorization

15. You are reviewing the design of an authentication system that uses EIGHT character passwords and has a password file where each entry is encrypted.

    Which of the following do you recommend adopting to provide the best protection against an attacker who can make multiple login attempts?

    A. Force users to use hard to guess passwords.
    B. Include a salt value when encrypting the passwords.
    C. Use a longer key.
    D. Use longer passwords.

    Idea here is get them to focus on the problem of bruteforcing from the console. Longer password -

16. Recognition by fingerprint, retina, and face are examples of:

    A. Dynamic biometrics.
    B. Face recognition.
    C. Static biometrics.
    D. Token authentication.

    Static biometrics

17. Which of the following describes the main defining feature of a *logic bomb*?

    A. Asorbs all of some class of resources.
    B. Propagated through sharing of USB sticks.
    C. Steals usernames and passwords.
    D. Triggered when some external event occurs.

    Triggered when some external event occurs

18. Evaluate whether the assertion given below is explained by the reason provided.

    Assertion: A signature-based anti-malware system may be able to detect files infected by a compression virus.

    Reason: Compression viruses modify the structure of the virus code to keep the size of the infected file constant.

    A. Both the assertion and the reason are true, and the reason is a correct explanation of the assertion.
    B. Both the assertion and the reasons are true, and the reason is NOT a correct explanation of the assertion.
    C. Both the assertion and reason are false.
    D. The assertion is true but the reason is false.

    The assertion and reason are true but the reason is not a correct explanation of the assertion.

19. Which of the following is the most desirable solution to the threat of malware?

    A. Detection.
    B. Identification.
    C. Prevention.

D. Removal.

Prevention

20. Which of the following protocols allow you to be able to determine the authenticity of the other party?
    A. HTTPS.
    B. WEP.
    C. WPA.
    D. WPA2.

HTTPS - certificates

21. Which of the following would NOT cause a *This Connection is Untrusted?* error to be displayed in a browser?
    A. Expired certificate.
    B. Fake certificate.
    C. Misconfigured server.
    D. SSL strip attack.

SSL strip attack.

22. What is the main purpose of an *IDS*?
    A. Act as a barrier between networks.
    B. Act as a trap for attackers.
    C. Identify attacks.
    D. Remove malware from PCs.

Identify attacks

23. What is a *true negative* in the context of an Intrusion Detection System?
    A. Intrusion-related activity identified as an intrusion.
    B. Intrusion-related activity identified as legitimate.
    C. Legitimate activity identified as an intrusion.
    D. Legitimate activity identified as legitimate.

Legitimate activity identified as legitimate

24. What is a vulnerability that allows criminals to inject scripts into web pages viewed by users?
    A. buffer overflow
    B. SQL injection
    C. XML injection
    D. Cross-site scripting

Cross-site scripting

25. What type of attack targets an SQL database using the input field of a user?
    A. Buffer overflow

B. SQL injection
C. XML injection
D. Cross-site scripting

SQL injection

26. Javascript is best known as an example of a _____ side language, whereas PHP is an example of a _____ side language.

Choose a pair below that would best complete the sentence above.

A. Client, Client.
B. Client, Server.
C. Server, Client.
D. Server, Server.

client, server

27. Consider HTML forms, GET sends the values as _____ whereas POST language sends them as _____.

Choose the pair below that would best complete the sentence above.

A. part of the HTTP response body, hidden within the HTTP request body.
B. HTML, as part of the HTTP request body.
C. query string parameters as part of the URL, HTML.
D. query string parameters as part of the URL, hidden within the HTTP request body.

query string parameters as part of the URL, hidden within the HTTP request body

28. Your application sets a cookie with the Secure attribute. What does this mean?

A. Client will send the cookie only over an HTTPS connection.
B. Cookie is set to read only by the browser.
C. The cookie cannot be accessed by Javascript.
D. The cookie will not be sent to another website.

Client will send the cookie only over an HTTPS connection

Social Engineering

29. *Phishing* relies primarily on which of the following techniques?

A. Blackmail.
B. Impersonation.
C. Shoulder surfing.
D. Tailgaiting.

Impersonation

30. What type of phishing targets high-value individuals?
    A. Email.
    B. Spear.
    C. Vishing.
    D. Whaling.

    Whaling

31. Which psychological experiment 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.

    Asch's experiment.

32. Which of the following is NOT an example of a social engineering attack?
    A. Phishing.
    B. Pretexting.
    C. Spamming.
    D. Tailgating.

    Spamming

33. In a phishing attack, what is the technology typically used to carry it out?
    A. Email.
    B. Operating systems.
    C. Surveillance camera.
    D. Wifi network.

    Email

34. The defining feature of a *quid pro quo* social engineering attack is?
    A. Benefit in exchange for information.
    B. Involves the victim in what they think is an illegal activity.
    C. Promise of an item that is desirable to the victim.
    D. Small outlay, large monetary reward.

    Benefit in exchange for information.

35. Which of the following social engineering attacks is considered to be a modern-day example of the *Spanish Prisoner scam*?
    A. 419 scam.
    B. Baiting.
    C. Invoice scam.
    D. Phishing emails.

    419 scam

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

    A. Database.
    B. Physical.
    C. Network.
    D. Web application.

Physical

37. Consider these parts of a *protection model*: deter, detect, alarm and respond.

    What part is missing?

    A. Deceive.
    B. Delay.
    C. Isolate.
    D. Recover.

Delay

38. Which of the following physical attacks requires a victim to enter the building ahead of the attacker?

    A. Break-in.
    B. Lockpicking.
    C. Piggybacking.
    D. Shoulder surfing.

Piggybacking

39. Which of these devices represents an example of physical access controls?

    A. Firewalls.
    B. Routers.
    C. Servers.
    D. Swipe cards.

swipe cards

40. Air conditioning, water system, and fire systems fall under which of the cybersecurity domains?

    A. Device.
    B. Network.
    C. Physical facilities.
    D. User.

physical facilities

41. The term describing the set of instructions and actions to be performed at every step in the incident response (IR) process is?

    A. Analysis steps.
    B. Playbook.
    C. Recovery manual.
    D. Response plan.

    Playbook

42. What is the main role of a security operations analyst (SOC)?

    A. Deploys tools and fixes.
    B. Manages access to systems.
    C. Manages the CSRIT activities.
    D. Monitors IDSes.

    .

    Monitors IDSes

43. Which of the following types of evidence can be used in a court case?

    A. Character.
    B. Circumstantial.
    C. Opinion.
    D. Oral.

    Circumstantial or Oral

44. A hard drive taken by investigators as part of an investigation contains a video file. The investigators copy the video file onto a USB stick that was stored in an unlocked drawer. Before presenting it to the court, they convert it to another format to allow viewing on a screen in the court room. During the trial the Judge says that it cannot be used.

    Which of the following statements is accurately describes why it is inadmissible?

    A. Conversion into another format.
    B. Copying from the hard drive to the USB.
    C. Chain of evidence cannot be guaranteed.
    D. All of the above.

    Chain of evidence cannot be guaranteed

    Ethics and legal aspects

45. What type of cybersecurity laws govern how an organization can share your sensitive data?

    A. Consumer guarantees.
    B. Non-repudation.
    C. Privacy.
    D. Secrecy.

    Privacy

46. Imagine that you have broken into a server to expose a crime against the New Zealand public. Unfortunately, you accidentally delete the records belonging to a legitimate business using the same remote server.

    What are the potential consequences under the Crimes Act 1961?

    A. Liable for a fine because loss occurred but life wasn't endangered.
    B. Liable for imprisonment because financial loss occurred.
    C. Nothing, although harm was done it was outweighed by the benefit to the public.
    D. Nothing, the deletion of the records was accidental and unintended.

    Liable for imprisonment

47. You have discovered a bug in a widely used and trusted computer system. The helpdesk for the company are unresponsive and you cannot find a disclosure policy on the website.

    What would be best practice to do next?

    A. Announce the vulnerability on twitter.
    B. Contact CERT NZ in the first instance.
    C. Email the company again asking for the bug to be fixed or else you will go the newspapers.
    D. Exploit the bug and publicise it at a hacker conference.

    Contact CERT NZ in the first instance

48. Which of the following is TRUE with respect to Bug Bounty schemes

    A. Participation is limited to professionals.
    B. Programming knowledge is required to be able to find bugs.
    C. Very few well-known companies offer bounties.
    D. Whoever finds and reports the bug first, will get paid.

    Whoever finds and reports the bug first, will get paid.

49. Evaluate the truth of the statement *cyberwarfare equals cyberwar*.

    A. False, only activists engage in cyberwarfare rather than nation states.
    B. False, cyberwarfare without involvement of other domains doesn't count as war.
    C. True, we have seen recently examples of nation states carrying out cyberwarfare.
    D. True, computers are integral to the conduct of modern wars.

    False, cyber attacks by themselves are not equivalent to warfare.

50. What type of offensive activity is *false news*?

    A. Espionage.
    B. Spamming.
    C. Subversion.
    D. Sabotage.

Subversion

SECTION B [15 marks]

- *Write answers in the spaces provided. If you write your answer elsewhere, make it clear where it can be found.*
- *The total for Section B is 15 marks. There are THREE questions worth FIVE marks each.*
- ***HAND IN this examination booklet.***

51. You have been employed to design a physical protection system to protect cash held by a cafe. The cafe has a single entrance off the street, a large open area where customers are served and an interior room with a lockable door that contains supplies and where the manager does their office work. Cash is kept in the cash register until the end of week when the manager takes it to the local bank for deposit.

    Recently there have been some overnight burglaries of stores in the same block of shops. The burglars not only stole money but caused a lot of damage to the stores because they used crowbars and sledgehammers to break into the shops and to access the cash within the shop. The damage caused is expensive and meant the stores could not open until the damage was repaired.

    (a) Briefly outline the the threat model that applies in this case.

    Aim of attacker is steal cash, attacker is a burglar who uses crowbars and sledgehammers to break into the building, they appear to have a low skill level as indicated by the damage done

    (b) Explain why you would not recommend installing a safe to store the cash overnight.

    The attackers do large amounts of expensive damage, if they cannot get into the safe they are likley to do more damage and the cost of this may outweigh the potential losses

(c) Propose an alternative approach based upon the protection model introduced in lectures.

It has to be something that doesn't cause worse damage. Examples - detect - cctv camera and obvious signs indicating that being recorded, alarm system for rapid response, perhaps do the banking every day so that there isn't cash left in the register and put a sign up indicating this.

52. A user rings the helpdesk reporting some odd internet banking transactions. You asked 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.

(a) What is *fundamental attribution error*?

Fundamental attribution error means people explain things by intentionality rather than situation.

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

Your friend would never intend to send you malware, therefore the malware could not have come from them.

53. You are employed as a Cyber Analyst and receive reports that the Cook Strait Ferry navigation system has been disabled by a cyber attack preventing it from sailing. Soon after the attack the newspapers are contacted by a group claiming it to be a Hacktivist group wanting publicity for their particular cause.

    (a) Explain why this could be considered *sabotage*.

Sabotage - cannot make a regular sailing

    (b) Explain why this is a *cyber attack* but not *cyberwarfare*?

Cyber warfare must be authorized by state actors in conjunction with a government campaign, this is a hacktivist group.

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