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

EXAMINATIONS – 2019

TRIMESTER 1 TERMS TEST

CYBR 171

CYBERSECURITY FUNDAMENTALS

Time Allowed: 50 minutes

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: Attempt **ALL** questions.

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.

Hand in the multi-choice answer sheet at the end.

SECTION A - CONCEPTS

All questions in this section are worth ONE mark.

1. Unauthorized modification of bank records is an example of a violation of:
    A. Availability.
    B. Confidentiality.
    C. Integrity.
    D. Privacy.

2. Someone falsely denying that they sent an email message is an example of a violation of:
    A. Authenticity.
    B. Authority.
    C. Non-repudiation.
    D. Usurpation.

3. The term *threat* describes:
    A. A measure of the extent to which an entity is threatened by a potential circumstance.
    B. Any event with the potential to adversely affect security of a system.
    C. Any kind of malicious activity attempting to disrupt, deny, degrade or destroy information resources.
    D. Weakness in a system that could be exploited by an attacker.

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

5. An attacker primarily interested in gaining publicity for a cause is most likely a:
    A. Black hat hacker.
    B. Cyber criminal.
    C. Hackivist.
    D. State-sponsored organization.

6. Which one of the following statements about designing a cryptographic algorithm is NOT true?

A. Details of the cipher algorithm must be kept secret.
B. Frequency analysis of the ciphertext should reveal as little as possible about the plaintext.
C. Long key lengths make it harder for attackers use a brute force attack.
D. Secrecy depends upon the key being kept secret.

7. Which one of the following statements about Private keys used with asymmetric cryptography is true?
   A. Can be used to calculate a matching public key.
   B. Can only be used to encrypt messages.
   C. Should be kept safe and never distributed.
   D. Should be sent to anyone wanting to exchange private encrypted messages with the owner of the key.

8. Which of the following symmetric cryptographic algorithms is MOST vulnerable to frequency analysis:
   A. Caeser cipher.
   B. One time pad.
   C. Pretty good privacy.
   D. Viginere cipher.

9. What is the MAIN problem solved by the Diffie-Hellman method?
   A. Authenticity of a key sent between communicating parties.
   B. Creating of keys resistant to brute force attacks.
   C. Large number of key pairs needed between communicating parties.
   D. Third party making a copy of a key sent between communicating parties.

10. Which of the following is used to produce a fingerprint of a file, message, or other block of data?
    A. Hash function.
    B. Digital signature.
    C. Keystream.
    D. Secret key.

11. Which of the following describes the process by which a system entity is granted a right or permission?
    A. Authentication.
    B. Authorisation.
    C. Identification.
    D. Non-repudiation.

12. Passwords are an example of which of the following common factors used for authentication?
    A. Something you are.
    B. Something you can do.
    C. Something you know.
    D. Something you possess.

13. Which of the following is best described as a software token?
    A. Google Authenticator.
    B. RSA SecureID
    C. NFC-enabled Credit Card.
    D. None of the above.

14. Which of the following statements most correctly describes two factor authentication?
    A. Always requires two unique passwords.
    B. Combination of something you know and something you possess.
    C. Relies upon the use of text messaging for security.
    D. Uses a special code that is never used twice and randomly generated.

15. Choose the option below that correctly orders biometric characteristics from least to most accurate?
    A. Face, Finger, Iris.
    B. Finger, Face, Iris.
    C. Finger, Iris, Face.
    D. Iris, Finger, Face.

16. Which of the following viruses were invented in Pakistan?
    A. Brain.
    B. Stoned.
    C. MacMag.

D. Peace.

17. Which of the following is a program with an overt purpose and a covert purpose?
    A. Bacteria.
    B. Logic bomb.
    C. Worm.
    D. Trojan.

18. Which of the following characteristics is unique to viruses?
    A. Exploits software vulnerabilities to propagate.
    B. Infect existing programs.
    C. Propagates across a network.
    D. Runs independently.

19. Compression viruses are designed to avoid detection by which of the following types of anti-virus systems?
    A. Heuristic-based detection.
    B. Integrity checkers.
    C. Signature-based detection.
    D. Sandboxing.

20. Which of the following is the best solution to the threat of malware?
    A. Detection.
    B. Identification.
    C. Prevention.
    D. Removal.

21. Who owns the Internet?
    A. Internet Task Force.
    B. No-one.
    C. USA.
    D. Vint Cerf.

22. Which of the following techniques can only protect SOME of your communications being eavesdropped upon by an attacker?
    A. HTTPS.

B. WEP.
C. WPA.
D. WPA2.

23. What does the browser plugin *HTTPS everywhere* do?
    A. Blocks non-HTTP websites.
    B. Enables HTTPS on a webserver.
    C. Redirects web browser to HTTPS version of the website.
    D. None of the above.

24. Which of the following is LEAST LIKELY to cause a "This Connection is Untrusted" error to be displayed in a browser?
    A. Expired certificate.
    B. Fake certificate.
    C. Fraudulently issued certificate.
    D. Misconfigured server.

25. Which of the following is an attack against WPA2?
    A. Krack.
    B. Petya.
    C. NotPetya.
    D. Slammer.

26. What is the main purpose of a firewall?
    A. Act as a barrier between networks.
    B. Act as a trap for attackers.
    C. Find PCs infected with malware.
    D. Identify attacks.

27. Which of the following policies can ONLY be implemented by an advanced firewall?
    A. Allow access to specific external web servers.
    B. Block malware inside the organisation attacking external machines.
    C. Prevent external attackers connecting to internal machines.
    D. Prevent traffic containing malware or sensitive information leaving the network.

28. Which of the following descriptions most closely describes a VPN?
    A. Anonymity for users.
    B. High speed connection.
    C. Reliable connection to a corporate network.
    D. Private connection across an untrusted network.

29. What is a *false 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.

30. Which of the following is a <u>WEAKNESS</u> of misuse detection as opposed to anomaly detection?
    A. Doesn't require regular updates.
    B. Less likely to raise false alarms.
    C. Misses new types of attack.
    D. Performance increases as add more rules.

SECTION B - PROBLEM SOLVING

All questions in this section are worth TWO marks.

Helpful note - The powers of two

N	2^N	N	2^N	N	2^N
1	2	11	2,048	21	2,097,152
2	4	12	4,096	22	4,194,304
3	8	13	8,192	23	8,388,608
4	16	14	16,384	24	16,777,216
5	32	15	32,768	25	33,554,432
6	64	16	65,536	26	67,108,864
7	128	17	131,072	27	134,217,728
8	256	18	262,144	28	268,435,456
9	512	19	524,288	29	536,870,912
10	1,024	20	1,048,576	30	1,073,741,824

31. You have been asked to encrypt the codeword *MORNING*.

    There are three possible one-time pads to consider to use:

    - *Pad A:* 2,9,1,4,7,2,10
    - *Pad B:* 3,9,2,9,5,0,9
    - *Pad C:* 10,5,6

    Which of the following statements is true?

    A. Pad A and C can be used but not Pad B because it repeats an offset more than once.

    B. Pad A and B can be used but not Pad C because it is too short.

    C. Pad A but not Pad B or Pad C for the reasons given above for each.

    D. None of the above.

32. Given a key length of 16 bits, calculate the AVERAGE number of keys that would have to be tried in a brute force attack to decipher an encrypted message.

    A. 16,384.

    B. 32,768.

    C. 65,536.

    D. 131,072.

33. Consider a computer system where passwords are stored using a *Salt and Hash* mechanism. Calculate the MAXIMUM time it would take to brute force a password under the following assumptions.

    - The password length is two characters.
    - The salt is one character.
    - Each character is stored as an 8-bit number.

- The authentication system allows you to try 10 attempts per second.
- We always round the answer up, i.e. 10.1 to 11.

A. 26 seconds.

B. 6,554 seconds.

C. 1,677,722 seconds.

D. 107,374,182 seconds.

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

Assertion: Asymmetric cryptography can provide confidentiality of data and non-repudiation by the sender.

Reason: Asymmetric cryptography uses longer keys than symmetric cryptography.

A. Both the assertion and reason are true, and the reason is a correct explanation of the assertion.

B. Both the assertion and reason 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.

35. Interpret the following firewall policy.

direction	Src IP	Src Port	Dst IP	Dst Port	Action
outbound	192.168.1.1	*	*	80	allow
inbound	*	*	192.168.1.1	>1023	allow
*	*	*	*	*	block

Which of the following rules does NOT apply:

A. Allows http and https traffic from any computer within the local area network to any web server.

B. Allows http traffic only from specific computer within the local area network to any web server.

C. Blocks https traffic from specific computer within the local area network to any web server.

D. Unless allowed, all other traffic is blocked entering or leaving the local area network.

****