TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI

VICTORIA

UNIVERSITY OF WELLINGTON

EXAMINATIONS – 2018

TRIMESTER 1

CYBR 171

CYBERSECURITY FUNDAMENTALS

Time Allowed: 120 MINUTES ******** 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.

Section A on pages 3 to 10 has 40 multi-choice questions.

The total for Section A is 40 marks.

Choose the best answer for each question in Section A and mark it on the mult-choice answer sheet provided.

Hand in the multi-choice answer sheet. **Your answers for Section A must be on the answer sheet, not in this question booklet.**

Section B on pages 11 to 15 has written answer questions.

The total for Section B is 40 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 [40 marks]

- *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.*
- *Each question is worth one mark, you do not lose marks for wrong answers.*

Fundamentals

1. What best describes a *passive* attack?

   A. Attempts to learn or make use of information from the system that does not affect system resources.

   B. Attempts to alter system resources or affect their operation.

   C. Initiated by an entity inside the security perimeter.

   D. Initiated from outside the perimeter.

   Attempts to learn or make use of information from the system that does not affect system resources.

2. Consider an attacker who obtains a copy of a list of credit card numbers from a web application, what security properties are being violated?

   A. Confidentiality.

   B. Availability.

   C. Integrity.

   D. Authorisation.

   Confidentiality

3. People (including your employees) are considered the weakest link in an information system. Which of the following best ensures security against employees of an organization?

   A. Intrusion Detection System.

   B. Assigning minimal access rights.

   C. Firewalls.

   D. Honeypots.

   Minimial access rights

4. Which of the following type of adversary is most likely to conduct sabotage, especially of real world facilities?

   A. Cyber criminals.

   B. Activists.

   C. State-sponsored organizations.

   D. Hobby hackers.

State-sponsored organizations

5. Digital signatures are used to detect the violation of which of the following security properties?

   A. Confidentiality.

   B. Availability.

   C. Integrity.

   D. Authorisation.

   integrity

6. Public keys can only be used to:

   A. Decrypt messages.

   B. Encrypt messages.

   C. Sign messages.

   D. Either decrypt or encrypt messages.

   Either decrypt or encrypt messages

7. One-time pads are provably secure as long as they:

   A. Do not contain english dictionary words.

   B. Are pseudorandom.

   C. Contain a mix of letters, numbers and special characters.

   D. Are truely random.

   are truely random

8. Four parties want to be able communicate securely with each other, they trust each other so only need to protect the confidentiality of their messages from external attackers. How many secret keys do they need assuming the use of symmetric cryptography?

   A. 1.

   B. 2.

   C. 6.

   D. 8.

   1 key only required, everyone can read everyone else's messages

   Authentication

9. Which of the following best describes the process by which a system entity provides a claimed identity to a system?

   A. Identification.

   B. Authentication.

   C. Authorisation.

   D. Non-repudiation.

   authentication

10. Which of the following authentication methods suffers from the problem that it is hard to revoke access once compromised?

    A. Something you know.

    B. Something you possess.

    C. Something you are.

    D. Something you can do.

    Something you are

11. Which of the following vulnerabilities *only* apply to software authentication tokens?

    A. Loss and theft.

    B. Prediction of the one time password.

    C. Infection by a virus.

    D. Forced downgrade.

    Infection by a virus

12. What approach provides protection of user passwords against both untrustworthy system administrators and hackers?

    A. Salt and hash.

    B. Shadow password files.

    C. Hypertext Transmission Protocol Secure (HTTPS).

    D. Symmetric cryptography.

    Salt and hash

    Malware and anti virus

13. Which of the following viruses were invented at Victoria University of Wellington?

    A. Brain.

    B. Stoned.

    C. Peace.

    D. MacMag.

    Stoned

14. A user calls you in a panic. He is receiving emails from people indicating that he is sending viruses to them. Over 200 such emails have arrived today. Which do you think is the cause?

    A. Bacteria virus.

    B. Logic bomb.

    C. Worm.

    D. Polymorphic virus.

    Worm

15. Which of the following types of anti-virus systems is likely to have the lowest false positive rate?

    A. Integrity checkers.

    B. Signature-based detection.

    C. Heuristic-based detection.

    D. Sandboxing.

    Signature-based detection

16. Which of the following types of anti-virus systems cannot detect *zero day exploits*?

    A. Integrity checkers.

    B. Signature-based detection.

    C. Heuristic-based detection.

    D. Sandboxing.

    Signature-based detection

    Network security

17. What aspect of the way that networks work is the *main reason* that communications between two people in the same country might be at risk of interception by another country's secret services?

    A. Submarine cables are at risk of being tapped.

    B. Packets can take any viable route between two users irrespective of distance.

    C. Users of public wirelness networks are vulnerable to eavesdropping.

    D. HTTPS is not used on all websites.

    Packets can take any viable route between two users irrespective of distance

18. You see the message ”This Connection is Untrusted” when browsing the web while connected to a public wireless network. What type of attack might be causing this?

    A. Packet sniffing.

    B. Evil twin.

    C. WEP decryption.

    D. KRACK.

    Evil twin

19. Which of the following attacks is a *protocol* denial-of-service attack?

    A. UDP flood.

    B. SYN flood.

    C. GET flood.

    D. Mail bomb.

    SYN flood

20. Which of the following attacks is an *application-level* denial-of-service attack?

    A. UDP flood.

    B. Ping of death.

    C. SYN flood.

    D. Slow Loris.

    Slow Loris

    Network defence

21. What aspect of the protection system model captures the intent of building Ruapekapeka in dense bush 15km from the sea?

    A. Deter.

    B. Detect.

    C. Alarm.

    D. Respond.

    Deter

22. What does the term *lateral movement* describe?

    A. Method used by an attacker to penetrate a network.

    B. Process of extracting confidential information from the network.

    C. How an attacker evades detection.

    D. Technique where attackers move from machine to machine within the network.

    Technique where attackers move from machine to machine within the network

23. Interpret the following firewall rule:

```
| direction | src      | dst      | protocol | dest port | action |
| in        | internal | external | tcp      | 25        | Permit   |
```

    A. Inbound mail from an external source is allowed.

    B. Inbound web connection to an external source is allowed.

    C. Outbound mail to an external source is allowed.

    D. Outbound web connection to an external source is allowed.

    Outbound mail to an external source is allowed

24. Which of the following technologies would be best for filtering web traffic?

    A. Packet filter.

    B. Stateful packet filter.

    C. Proxy gateway.

    D. Intrusion detection system.

    Proxy gateway

    IDS

25. Which of the following is most likely to be considered cyberwarfare?

    A. Anonymous carry out a denial-of-service attack on a government website.

    B. Company sabotages rival company based on a enemy country.

    C. Army unit steals state secrets from enemy country.

    D. State sponsored hackers sabotage elections held by enemy country.

    State sponsored hackers sabotage elections held by enemy country

26. Which of the following Intrusion Detection System (IDS) types looks for unusual activity?

    A. Signature based.

    B. Misuse based.

    C. Anomaly based.

    D. Difference based.

    Anomaly based

27. What typically happens as the number of rules in a signature database grows?

    A. False positives decrease.

    B. Performance degrades.

    C. False negatives increase.

    D. Performance increases.

    Performance degrades

28. What type of Intrusion Detection System (IDS) is SNORT?

    A. Signature-based host intrusion detection system.

    B. Anomaly-based host intrusion detection system.

    C. Signature-based network intrusion detection system.

    D. Anomaly-based network intrusion detection system.

    Signature-based network intrusion detection system.

29. An Intrusion Prevention System (IPS) is typically built by combining an Intrusion Detection System (IDS) with which of the following component?

    A. Personal firewall.

    B. Anti virus.

    C. Router.

    D. Honeypot.

    Router

    Social engineering

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

    A. Shoulder surfing.

    B. Tailgaiting.

    C. Blackmail.

    D. Impersonation.

31. What type of phishing targets high value individuals?

    A. Email.

    B. Whaling.

    C. Spear.

    D. Vishing.

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

33. Which of the following security techniques helps protect users against social engineering attacks?
    - A. OWASP.
    - B. OSINT.
    - C. OPSEC.
    - D. PSYOPS.

    OPSEC

34. Which of the following terms best describes the behaviour when we go for the ”good enough” option?
    - A. Affect heuristic.
    - B. Risk avoidance.
    - C. Satisficing.
    - D. Prospect theory.

    Satisficing

    Incident handling and response

35. The term describing the set of instructions and actions to be perfromed at every step in the incident response (IR) process is?
    - A. Response plan.
    - B. Analysis steps.
    - C. Playbook.
    - D. Recovery manual.

36. Which of the following terms best describe computer forensics?
    - A. Study of how cyber crimes are committed.
    - B. Allows future crimes to be prevented.
    - C. Recovery and investigation of material found in digital devices.
    - D. Conducted primarily by lawyers.

37. Which of the following main types of evidence is not admissable unless *by leave of the court*.
    - A. Oral.
    - B. Similar fact.
    - C. Secondary.
    - D. Circumstantial.

Similar fact

Application security

38. Which attack can execute Javascript in the user's browser?

    A. SQL injection

    B. Cross site scripting

    C. Malware uploading

    D. Man in the middle

Cross site scripting

39. Which attack can be used to execute attacker instructions on the victim's server?

    A. SQL injection

    B. Cross site scripting

    C. Main the middle

    D. Cookie stealing

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

    A. The cookie cannot be accessed by Javascript.

    B. The cookie will not be sent to another website.

    C. Client will send the cookie only over an HTTPS connection.

    D. Cookie is set to read only by the browser.

SECTION B [40 marks]

41. **Cryptography.** Briefly describe the main differences between ECB and CBC cipher mode? **(4 marks)**

It is the simplest mode of encryption. Each plaintext block is encrypted separately. Similarly, each ciphertext block is decrypted separately. In a CBC mode, instead of just processing each block separately, every block will be combined with the encrypted previous block. This effectively means that every block depends on the output of the previous block.

42. **Authentication.** Explain why simply storing passwords encrypted using a strong encryption algorithm with a single large 1024 sized key is not recommened and how you could improve the design. **(4 marks)**

Using a single key and encryption algorithm results in same encrypted passwords for users who have selected a specific password.The compromise of a single password result in the compromise of many other accounts. Countermeasure is salt and hash. Inclusion of salt means that every password entry (now a hash) is different. NOTE that the ecnryption is strong so we aren't worried about brute forcing the ciphertext here and reversing the encryption.

43. **Malware and anti vius.** Explain the concept of polymorphic malware, how do they differ compared to traditional malware and the methods used by antivirus detection engines to detect them. **(4 marks)**

A polymorphic malware mutates and evolves over time, creating copies of itself that have different characteristics to other copies while the main functionality remains the same. They changes the way they appear to antivirus software programs making them undetectable by techniques that look for preconfigured signatures or patterns. Since only the signature of the virus changes and not its behaviour, antivirus software can detect all the variants by identifying and blocking the behavior that malware exhibit and rely on to execute on a host system.

44. **Network security attacks.** Explain how a DDoS attack using an amplification techniques work. **(4 marks)**

Many servers used in amplification attacks are either public servers (e.g. DNS servers) or currently sit exposed online with no authentication protection, meaning an attacker can access them and send them a special command packet that the server will respond to with a much larger reply. Attackers simply spoof the IP address of their victim and send small queries to multiple servers. The systems then return much larger requests back to the victim.

45. **Defensive technologies.** Outline why is it critically important to define the goal of a protection system and the main components of a threat model. **(4 marks)**

Cannot protect everything, too expensive so must choose what is most important to protect. Threat model composed of understanding the attacker's motives, their level of skill and equipment that they might have to use in an attack.

46. **Intrusion detection.** How does a false positive alarm differ from a false negative one? From a security perspective, which is least desirable? **(4 marks)**

A false positive seems like an alert, but is in fact, routine activity. A false negative seems like normal activity and is in fact an alert-level action. From a security viewpoint, it depends upon the nature of the system being protected. Under some circumstances a high rate of false positives might lead to operator fatigue and missing of real attacks while high rates of false negatives mean that a significant attack is missed.

47. **Social engineering.** Compare *pretexting* and *phishing* attacks in terms of their targets and their methods. **(4 marks)**

Pretexting attacks focus on the organisation and involves impersonating a person with legitimate access to information. Phishing targets individuals and involve impersonating usually an organisation.

48. **Incident handling and recovery.** Briefly outline the main benefits of preparing an incident response plan prior to a cyber attack. **(4 marks)**

No time during cyber attack to respond, reasons being difficulty to both determine what is happening and under pressure from users and manager. Allows orderly response - limit damage of attack, recover from potential damage.

49. **Digital forensics.** Briefly explain why a *trace* is always a form of secondary evidence and why it is important with digital forensics to collect multiple traces. **(4 marks)**

Trace is formed by an object coming into contact with another one (Locard's exchange principles). This means that we don't have the original piece of evidence. These traces are easy to forge in a digital environment. Multiple traces makes this harder to do because they can be compared to each other.

50. **Application security.** Briefly explain why when performing *certain* critical tasks on some websites you are asked to reauthenticate yourself. **(4 marks)**

Cross site request forgery where user tricked into executing an unwanted action on a trusted site. Forcing user to reauthenticate highlights that this action is taking place and gives user opportunity to cancel the action. Not done for all actions because this would annoy the user and affect the usability of the site.

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