1.6 Network Security: 30-minute Pack

OCR J277 · Calculators not allowed · about 30 minutes

Total Marks

Name: _____ Date: ____ / ____ / _____

Answer ALL questions. Show all your working.

1 A cafe offers customers a wireless network.

(a) State one reason why an unencrypted (open) wireless network is a greater security risk than a wired network. **(1)**

(b) State the name of a protocol that could be used to encrypt traffic on the cafe's wireless network, and give one reason why using it is preferable to leaving the network open. **(2)**

(Total for Question 1 is 3 marks)

2 Every device on a network is identified, in part, by its IP address and MAC address.

(a) One octet of an IPv4 address has the denary value 182. Convert 182 to an 8-bit binary number. **(2)**

(b) Part of a device's MAC address is written in hexadecimal as 2F. Convert 2F to an 8-bit binary number. **(2)**

(c) Convert 2F (hexadecimal) to a denary number. **(1)**

(Total for Question 2 is 5 marks)

© Revision Library | revisionlibrary.co.uk

3 State three different physical security measures that an organisation could use to protect the server room containing its network hardware. For each measure, justify why it helps to keep the servers secure.

(Total for Question 3 is 6 marks)

---

4 A secondary school's network is regularly targeted by malware, often arriving as attachments in phishing emails sent to staff and students.

Discuss the effectiveness of anti-malware software and staff/student training as methods of protecting the school's network against malware threats. In your answer you should consider the strengths and weaknesses of each method, and reach a justified conclusion about which is likely to be more effective.

(Total for Question 4 is 6 marks)

© Revision Library | revisionlibrary.co.uk

5 Write an algorithm, using pseudocode, that could be used to control access to an account, as follows:

- the correct password is already stored in a variable called realPassword
- the user is asked to enter a password
- the user is allowed up to 3 attempts in total
- if the user enters the correct password within 3 attempts, the algorithm should output "Access granted" and stop asking for a password
- if the user has still not entered the correct password after 3 attempts, the algorithm should output "Account locked"

You may use any valid pseudocode. Marks will be awarded for correct logic; minor syntax errors will not be penalised.

(Total for Question 5 is 6 marks)

6 A company director states: "As long as we encrypt all the data stored on our network, our network will be secure."

Evaluate this statement.

(Total for Question 6 is 6 marks)

© Revision Library | revisionlibrary.co.uk

Mark scheme · 1.6 Network Security: 30-minute Pack

Question 1

(a) Any nearby device can intercept/eavesdrop on the wireless signal without needing physical access to the cabling, because data travels through the air and can be picked up by anyone in range — **B1**

(a) Answer: Data sent over an open wireless network can be intercepted by any device within range, without needing physical access to network cables.

(b) WPA (or WPA2 or WPA3) named — **B1**

(b) Encrypts data sent over the wireless network so it cannot easily be read/understood if intercepted by an attacker — **B1**

(b) Answer: WPA2 (or WPA3); it encrypts wireless traffic so intercepted data cannot easily be read by an attacker.

Question 2

(a) Correct method shown, e.g. 128+32+16+4+2 = 182 or place-value table attempted — **M1**

(a) 10110110 cao — **A1**

(a) Answer: 10110110

(b) 2 -> 0010 and F -> 1111 (nibbles identified/attempted) — **M1**

(b) 00101111 cao — **A1**

(b) Answer: 00101111

(c) 47 cao (ft from (b) if binary answer evaluated consistently) — **B1**

(c) Answer: 47

Question 3

Measure 1, e.g. keycard/biometric access lock on the server room door — **B1**

Justification 1, e.g. only authorised staff whose card/fingerprint is registered can enter, preventing unauthorised physical access — **B1**

Measure 2, e.g. CCTV cameras covering the server room — **B1**

Justification 2, e.g. records who enters/leaves and can deter, or help identify, anyone attempting unauthorised access — **B1**

Measure 3, e.g. security guards/visitor sign-in log at the building entrance, or locked server cabinets/cages — **B1**

Justification 3, e.g. ensures only checked/verified individuals can reach the area containing the server room — **B1**

Answer: Any three distinct physical security measures (e.g. keycard/biometric locks, CCTV, security guards, locked server cabinets, alarmed doors), each with a valid justification.

Question 4

Level 1 Basic, undeveloped comments about anti-malware software and/or staff training are given, with little or no comparison. Little relevant technical terminology is used. No conclusion, or an unsupported conclusion. — **1-2**

Level 2 Some relevant strengths and/or weaknesses of both methods are described, showing some understanding of how each works. Some comparison is attempted, but the discussion may be one-sided or lack detail in places. Relevant technical terminology is generally used correctly. A conclusion is given, with limited justification. — **3-4**

Level 3 A well-balanced discussion clearly describes strengths and weaknesses of both anti-malware software and staff training, showing clear understanding of how each reduces the risk of malware infection and the limitations of each. Relevant technical terminology is used correctly throughout. A justified conclusion is reached that is well supported by the points made. — **5-6**

Indicative content:

- Anti-malware software can automatically scan files/emails/attachments and detect or quarantine known malware using a database of virus definitions/signatures
- Anti-malware software needs to be regularly updated to recognise new malware; it may not detect brand new (zero-day) malware whose signature is not yet known
- Anti-malware runs continuously/automatically without relying on staff remembering to act, so it protects against mistakes even when staff are careless
- Staff/student training teaches users to recognise suspicious emails/attachments/links (e.g. unexpected sender, spelling mistakes, urgent requests) and not to open or click them
- Training relies on human behaviour, which is not always reliable; a single tired, rushed or careless user can still open a malicious attachment even after training
- Training does not stop malware that arrives through other routes (e.g. infected USB sticks, software vulnerabilities) that do not require a user to be tricked
- The two methods are complementary: anti-malware provides a technical safety net, while training reduces the number of malicious emails opened in the first place
- A justified conclusion might state that using both together is most effective, since anti-malware alone cannot stop all new threats and training alone cannot guarantee human error is eliminated

© Revision Library | revisionlibrary.co.uk

Question 5

Uses a loop (e.g. WHILE or FOR) that will not run more than 3 times in total	**M1**
Inputs a password from the user inside the loop, on each pass	**M1**
Compares the entered password to realPassword	**M1**
Correctly counts/tracks the number of incorrect attempts (e.g. increments a counter only when incorrect, or an equivalent valid method)	**M1**
Stops asking for further passwords and outputs "Access granted" as soon as a correct password is entered (within the 3 attempts)	**M1**
Outputs "Account locked" if, and only if, 3 incorrect attempts have been made	**M1**

Answer:

```
realPassword <- "Sunfl0wer"
attempts <- 0
accessGranted <- FALSE
WHILE attempts < 3 AND accessGranted = FALSE
  password <- INPUT("Enter password: ")
  IF password = realPassword THEN
    accessGranted <- TRUE
  ELSE
    attempts <- attempts + 1
  ENDIF
ENDWHILE
IF accessGranted = TRUE THEN
  OUTPUT "Access granted"
ELSE
  OUTPUT "Account locked"
ENDIF
```

Question 6

Level 1 A basic, one-sided response that only considers what encryption does, with little or no reference to other threats. Little or no use of relevant technical terms.	**1-2**
Level 2 The response explains what encryption protects against, and identifies at least one other type of threat that encryption does not prevent, but the argument is not fully developed or the two sides are not clearly linked to a conclusion.	**3-4**
Level 3 A well-developed evaluation clearly explains what encryption protects against and identifies several other categories of threat (e.g. malware, social engineering, physical access, poor access control) that encryption does not prevent, and reaches a clear, justified conclusion about whether the statement is correct. Technical terminology is used accurately throughout.	**5-6**

Indicative content:

- Encryption protects the confidentiality of data: if data is intercepted (e.g. during transmission) or a storage device is stolen, it cannot be read/understood without the correct key
- Encryption does not stop malware (viruses, worms, trojans, ransomware) infecting the network and disrupting or destroying data/systems
- Encryption does not stop social engineering attacks (phishing, blagging, shouldering, pharming) that trick a user into revealing a password or other information, which could then be used to access even encrypted data legitimately
- Encryption does not stop a denial-of-service attack, which prevents legitimate users from accessing services regardless of whether the data is encrypted
- Encryption does not control who is allowed to access which data on the network (this requires user access levels/permissions), or prevent unauthorised physical access to hardware
- Encrypted data can still be deleted, corrupted or held to ransom, so encryption alone does not guarantee the availability or integrity of data, only its confidentiality
- A justified conclusion should recognise that encryption is one useful, valid layer of protection (particularly for confidentiality) but is not sufficient on its own; a combination of measures (encryption, anti-malware, firewalls, access levels, training, physical security) is needed for a network to be considered secure

© Revision Library | revisionlibrary.co.uk