1.6 Network Security: Test Pack

OCR J277 · Calculators not allowed · about 25 minutes

Total Marks

Name: _____ Date: ____ / ____ / _____

Answer ALL questions. Show all your working.

1 This question is about basic network security terminology.

(a) Which term describes software that is deliberately designed to damage, disrupt or gain unauthorised access to a computer system? **(1)**

- ☐ A) Firmware
- ☐ B) Malware
- ☐ C) Freeware
- ☐ D) Middleware

(b) Which type of malware can replicate itself and spread across a network without attaching itself to another program or needing a user to run it? **(1)**

- ☐ A) Virus
- ☐ B) Worm
- ☐ C) Trojan
- ☐ D) Spyware

(c) Which type of attack involves tricking a user into revealing personal or financial information by pretending to be from a genuine, trustworthy organisation (e.g. in a fake email)? **(1)**

- ☐ A) Brute force
- ☐ B) Denial of service
- ☐ C) Phishing
- ☐ D) SQL injection

(Total for Question 1 is 3 marks)

© Revision Library | revisionlibrary.co.uk

2 A website's login page checks a user's credentials using the following line of code, which builds an SQL query from the text entered into the username and password boxes:

```
SELECT * FROM users WHERE username = 'INPUT_USERNAME' AND password = 'INPUT_P
```

An attacker enters the following into the username box, leaving the password box empty:

' OR '1'='1

(a) Identify the type of attack the code above is vulnerable to. **(1)**

(b) Explain how entering ' OR '1'='1 into the username box could allow the attacker to log in without knowing a valid username or password. **(2)**

(c) State one method a web developer could use to help prevent this type of attack. **(1)**

(Total for Question 2 is 4 marks)

© Revision Library | revisionlibrary.co.uk

3 Encryption is used to protect data sent across a network.

(a) Explain what is meant by encryption, and why it is used to protect data sent over a network. **(3)**

(b) A simple cipher encrypts a message by shifting every letter 3 places forward in the alphabet (wrapping around, so X->A, Y->B, Z->C). Show that encrypting the plaintext WIFI using this cipher produces the ciphertext ZLIL. **(2)**

(c) State one weakness of this shift cipher compared to modern encryption methods used on networks. **(1)**

(Total for Question 3 is 6 marks)

© Revision Library | revisionlibrary.co.uk

4 Four employees at a company called Hartlepool Logistics describe problems with their work computers. For each description, name the most likely type of malware responsible. Choose from: virus, worm, trojan horse, ransomware.

(a) Priya's files have all been encrypted and a message on her screen demands payment in exchange for the decryption key. **(1)**

(b) Deshawn downloaded a free game from an unofficial website. The game appeared to work normally, but it secretly installed a program that now lets an attacker access his files remotely. **(1)**

(c) Overnight, the same malicious program appeared on every computer on the office network, without any employee opening a file or clicking a link. **(1)**

(d) Aisha noticed her computer running slowly after opening an email attachment; the same corrupted code was then found attached to several of her other documents. **(1)**

(Total for Question 4 is 4 marks)

---

5 Explain how giving employees different user access levels can reduce the risk of an insider threat compromising sensitive data on a company's network.

(Total for Question 5 is 3 marks)

© Revision Library | revisionlibrary.co.uk

Mark scheme · 1.6 Network Security: Test Pack

Question 1

(a) B cao **B1**

(a) Answer: B) Malware

(b) B cao **B1**

(b) Answer: B) Worm

(c) C cao **B1**

(c) Answer: C) Phishing

Question 2

(a) SQL injection **B1**

(a) Answer: SQL injection

(b) The entered text changes/completes the structure of the SQL query so that the condition '1'='1' is added into the WHERE clause (1) **M1**

(b) Because '1'='1' is always true, the whole WHERE condition becomes true for every row, so the query returns a user record even though no correct username/password was supplied (1) **A1**

(b) Answer: It alters the query so the WHERE condition is always true, so the database returns a valid user row without a correct username/password being entered.

(c) Any one of: use parameterised queries/prepared statements; validate/sanitise user input; escape special characters (e.g. apostrophes) entered by the user; use least-privilege database accounts **B1**

(c) Answer: Use parameterised queries (prepared statements) so user input cannot be interpreted as SQL code.

Question 3

(a) Encryption converts data (plaintext) into an unreadable/scrambled form (ciphertext) using an algorithm and a key (1) **B1**

(a) If the data is intercepted while being transmitted, it cannot be understood/read by the attacker (1) **B1**

(a) Only someone with the correct key can decrypt the data back into its original readable form (1) **B1**

(a) Answer: Encryption scrambles data into ciphertext using a key so that, if intercepted, it cannot be understood; only someone with the correct key can decrypt it back to plaintext.

(b) At least two letters correctly shifted with working shown, e.g. W(+3)->Z, I(+3)->L **M1**

(b) All four letters correctly shown: W->Z, I->L, F->I, I->L, giving ZLIL cso **A1**

(b) Answer: ZLIL (answer given in question; working must be shown)

(c) Any one of: only 25 possible shifts/keys so it can quickly be broken by trying every shift (brute force); the pattern/frequency of letters is unchanged so it is vulnerable to frequency analysis; it does not use a complex/long key like modern encryption algorithms **B1**

(c) Answer: It only has 25 possible keys (shifts), so an attacker could try every shift and break it very quickly by brute force.

Question 4

(a) Ransomware **B1**

(a) Answer: Ransomware

(b) Trojan (horse) **B1**

(b) Answer: Trojan horse

(c) Worm **B1**

(c) Answer: Worm

(d) Virus **B1**

(d) Answer: Virus

Question 5

Different user accounts/groups are given different permissions (e.g. read-only, read/write, administrator) depending on their role (1) **B1**

Employees can only access/view/edit the data and systems that they need for their job, not the whole network (1) **B1**

This limits the amount of damage/data an employee could deliberately or accidentally misuse, and makes it easier to trace which account accessed particular data (1) **B1**

Answer: Access levels restrict each employee to only the data/systems needed for their role, limiting the damage any one account could cause and making misuse easier to trace.

© Revision Library | revisionlibrary.co.uk