

End of topic quiz

FIRST ASSESSMENT
SUMMER 2022

Topic 1.4 Network security

1.

a. Which **two** boxes are malware?

	Tick (✓)
Sandboxing	
Rootkit	
NAT router	
Key logger	

b. What are **two** methods that could be used to infect a laptop with malware?c. What are **two** types of anti-malware that should be used to protect a laptop?

2.

a. How could phishing take place at a business?

b. What are **two** potential problems to a business if phishing takes place?

c. Describe **one** other example of social engineering that employees at a business should be aware of.

3.

a. What is meant by the term 'brute-force attack'?

b. What are **four** features of a strong password?

c. What are **two** measures in addition to a password that could be used to keep a computer's data secure?

4.

- a. What are **three** reasons why companies may be targeted by a denial of service attack?

--

- b. What are **two** measures that a company could take to prepare for a denial of service attack?

--

5. It is important that all users of a computer network realise what they can and cannot access on the network. The **table** below lists some actions that a student, a tutor and a network manager have authority to perform on a school network.

Which action(s) should a student, a tutor and, or a network manager be able to perform?

Action	Student	Tutor	Network manager
Change system settings			
Access a shared area for students			
Add or delete network users			
Access the student's file and make changes to it			
Access a shared area for tutors			
Install software			

COMPUTER SCIENCE

6. Josh works in the finance department of a council. He has been asked by his manager to email an important document containing personal and financial information to Saida. Saida works at a firm of accountants located in another part of the country.

- a. What is **one** method that a business could use to ensure that sensitive documents will not be read by anyone except the intended recipient?

- b. What is the plain text for this cipher when a Caesar cipher is used?

XLI HEXE MW WIGYVI

- c. The **table** below lists three statements. Which statements are **True** and **False**?

Statement	True	False
The Caesar cipher is an example of a substitution cipher.		
A private key can be made available to everyone.		
Advanced Encryption Standard uses 128-bit, 192-bit or 256-bit keys.		

7.

- a. What are **four** reasons why an attacker might want to target an organisation's database with an SQL injection?

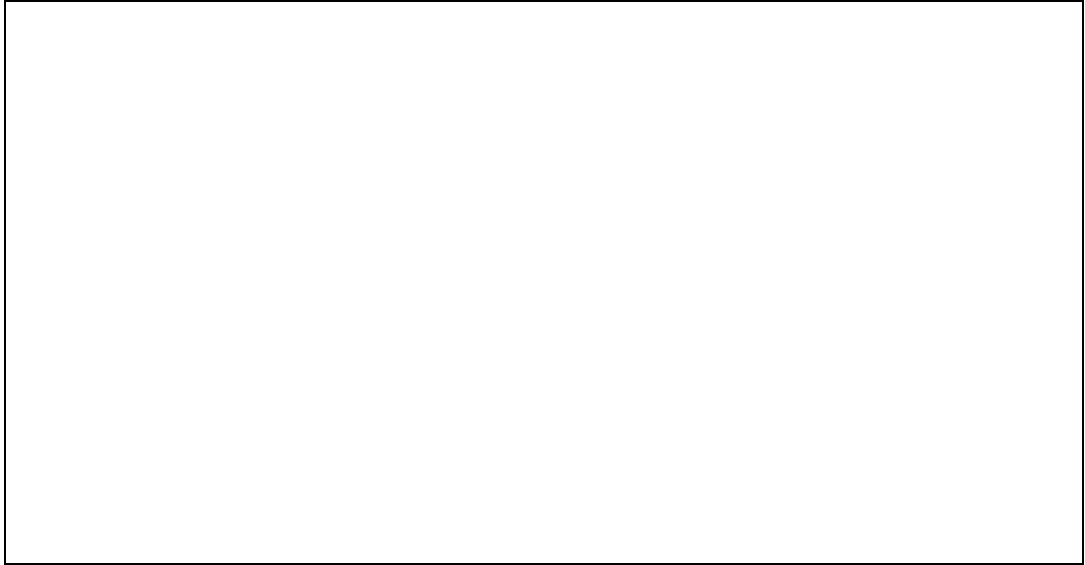
- b. What are **two** measures that an organisation should take to guard their software applications from an SQL injection attack?

8.

- a. What are **two** advantages of using a firewall?

- b. Give a comparison of intrusion detection and vulnerability testing.

- c. How penetration testing helps secure the telecommunication company's computer network.



9. What are **four** ways of physically protecting a network?



Answers

1.

- a. The list below contains two types of malware. Tick **two** boxes to identify the two types of malware.

Malware	Tick (✓)
Sandboxing	
Rootkit	✓
NAT router	
Key logger	✓

- b. What are **two** methods that could be used to infect a laptop with malware?

- Software that was installed from an untrustworthy source, for example, screensavers, etc.
- Existing anti-malware software is out of date
- Out of date system software/application software
- Out of date browser
- Out of date firewall
- Infected removable drives
- Exploitation of a software vulnerability
- Various social engineering techniques, e.g. phishing
- Scareware
- Infected email attachment
- Infected link
- Spam email
- A hacked website
- Fake website
- Popup software
- Illegal file sharing
- Distributed denial of service
- Adware
- Rootkits

c. What are **two** types of anti-malware that should be used to protect a laptop?

- Anti-virus
- Anti-spyware
- Malware scanner

2.

a. How could phishing take place at a business?

- Staff respond to fake email
- Staff respond to fake link
- Staff respond to fake website
- Staff respond to spam
- Staff respond to popup software fake instant messages
- Staff respond to social media messages, 'likes', etc.

b. What are **two** potential problems to a business if phishing takes place?

- Acquisition of user names and passwords
- Acquisition of financial details/credit card details
- Identity theft
- Data theft
- Staff disclose personal/confidential data
- Financial data theft

c. Describe **one** other example of social engineering that employees at a business should be aware of.

- Pharming
- Blagging/pre-texting
- Shoulder surfing
- Baiting scenarios
- Countermeasures
- Tailgating
- Quid-pro-quo
- Hoax viruses

3.

a. What is meant by the term 'brute force attack'?

- An attack that attempts to decode passwords/encryption keys/encrypted data
- All possible/numerous combinations are attempted
- A trial and error method
- Resource/time consuming method

b. What are **four** features of a strong password?

- At least eight characters
- Include upper case
- Include lower case
- Include special characters
- Include numbers
- Does not include a name, company name or user name
- Does not contain a complete word
- Relates to an acronym

c. What are **two** measures in addition to a password that could be used to keep a computer's data secure?

- Encryption/encrypt data
- Set a PIN/pattern to lock the phone
- Install security software
- Download apps from trusted sources
- Keep the operating software and apps updated
- Log out of sites
- Turn off automatic Wi-Fi connection
- Turn off Bluetooth and NFC when not in use
- Biometrics

4.

a. What are **three** reasons why companies may be targeted by a denial of service attack?

- Protest/hacktivism
- Cyber vandalism
- Distraction technique
- Espionage – commercial, industrial, political
- Can lead to malware/data theft if part of a distraction technique
- If a distributed denial of service attack can lead to computer/network control
- Extortion
- Competition between companies
- Make a website unavailable
- Interrupt an organisation's work
- Suspend an organisation's work
- Block user requests

b. What are **two** measures that a company could take to prepare for a denial of service attack?

- Networks should be monitored
- Penetration testing should be undertaken/vulnerabilities should be found
- Vulnerabilities should be fixed/remedied
- A response plan should be produced
- Proxy servers and firewalls

COMPUTER SCIENCE

5. It is important that all users of a computer network realise what they can and cannot access on the network. The **table** below lists some actions that a student, a tutor and a network manager have authority to perform on a school network.

Which action(s) should a student, a tutor and, or a network manager be able to perform?

Action	Student	Tutor	Network manager
Change system settings			✓
Access a shared area for students	✓		
Add or delete network users			✓
Access the student's file and make changes to it	✓		
Access a shared area for tutors		✓	
Install software			✓

6. Josh works in the finance department of a council. He has been asked by his manager to email an important document containing personal and financial information to Saida. Saida works at a firm of accountants located in another part of the country.

- a. What is **one** method that a business could use to ensure that sensitive documents will not be read by anyone except the intended recipient?

Encryption.

- b. What is the plain text for this cipher when a Caesar cipher is used?

XLI HEXE MW WIGYVI

The data is secure.

c. The **table** below lists three statements. Which statements are **True** and **False**?

Statement	True	False
The Caesar cipher is an example of a substitution cipher.	✓	
A private key can be made available to everyone.		✓
Advanced Encryption Standard uses 128-bit, 192-bit or 256-bit keys.	✓	

7.

a. What are **four** reasons why an attacker might want to target an organisation's database with an SQL injection?

- Access sensitive data
- Steal/retrieve personal data
- Access/steal/retrieve financial data
- Create/read/update/modify/delete data
- Destroy data
- Take control of data

b. What are **two** measures that an organisation should take to guard their software applications from an SQL injection attack?

- Limit user access/privileges
- Create user accounts
- Apply input sanitation
- Apply an input validation technique
- Apply patches/software updates
- Install web application firewall/strong web application firewall

8.

a. What are **two** advantages of using a firewall?

- Controls network traffic/allows data from authorised
- Blocks data from unauthorised sources
- Protects against attackers
- Offers different protection levels
- Protects privacy
- Provides warnings
- Filters advertisements/popups
- Filters web content

b. Give a comparison of intrusion detection and vulnerability testing.

- Intrusion detection monitors a network for unauthorised access by an attacker.
- Intrusion detection identifies unauthorised access after an attacker has breached a network's security.
- Vulnerability testing scans a network for vulnerabilities.
- Vulnerability testing detects vulnerability before an attack occurs.

c. How penetration testing helps secure the telecommunication company's computer network.

- Penetration testing looks for vulnerabilities.
- It attempts to exploit the vulnerabilities that it finds.
- The results of penetration testing are presented to network managers to help them to remedy the vulnerabilities
- It helps to protect a system from cyber attacks
- It identifies and prioritises security risks
- It helps to save money/resources
- It helps to avoid down time
- It helps to protect a company's reputation

9. What are **four** ways of physically protecting a network?

- Door locks
- Window locks or bars
- Intruder alarm systems
- CCTV systems
- Laptop locks (e.g. Kensington locks)
- Security guards

We'd like to know your view on the resources we produce. By clicking on '[Like](#)' or '[Dislike](#)' you can help us to ensure that our resources work for you. When the email template pops up please add additional comments if you wish and then just click 'Send'. Thank you.

If you do not currently offer this OCR qualification but would like to do so, please complete the Expression of Interest Form which can be found here: www.ocr.org.uk/expression-of-interest

OCR Resources: *the small print*

OCR's resources are provided to support the delivery of OCR qualifications, but in no way constitute an endorsed teaching method that is required by the Board, and the decision to use them lies with the individual teacher. Whilst every effort is made to ensure the accuracy of the content, OCR cannot be held responsible for any errors or omissions within these resources.

Our documents are updated over time. Whilst every effort is made to check all documents, there may be contradictions between published support and the specification, therefore please use the information on the latest specification at all times. Where changes are made to specifications these will be indicated within the document, there will be a new version number indicated, and a summary of the changes. If you do notice a discrepancy between the specification and a resource please contact us at: resources.feedback@ocr.org.uk.

© OCR 2020 - This resource may be freely copied and distributed, as long as the OCR logo and this message remain intact and OCR is acknowledged as the originator of this work. OCR acknowledges the use of the following content: n/a
Please get in touch if you want to discuss the accessibility of resources we offer to support delivery of our qualifications: resources.feedback@ocr.org.uk