End of Unit Quiz – Unit 1.6 System Security

1.

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

Malware	Tick (✔)
Sandboxing	
Zombie	
NAT router	
Key logger	

    b. What are **two** methods that could have been 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 call centre?

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

   c. Describe **one** other example of social engineering that employees at the call centre 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.

   Tick **one** box in each row to show which action a student, a tutor and a network manager are authorised to undertake.

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, who 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. Convert this cipher text into plain text.

XLI HEXE MW WIGYVI

c. The **table** below lists three statements. Tick **one** box in each row to show whether a statement is **True** or **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?

> [blank answer box]

8.

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

> [blank answer box]

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

> [blank answer box]

c. Write about how penetration testing helps secure the telecommunication company's computer network.

> [blank answer box]

Answers

1.

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

Malware	Tick (✔)
Sandboxing	
Zombie	✔
NAT router	
Key logger	✔

b. What are **two** methods that could have been 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 call centre?

- 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 call centre 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 the call centre should be aware of.

- Pharming
- Blagging/pre-texting
- Shoulder surfing
- Baiting scenarios
- Countermeasures
- Tailgating
- Responses to fictitious s
- 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

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

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.

Tick **one** box in each row to show which action a student, a tutor and a network manager are authorised to undertake.

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, who 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. Convert this cipher text into plain text.

XLI HEXE MW WIGYVI

The data is secure.	

c. The **table** below lists three statements. Tick **one** box in each row to show whether a statement is **True** or **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. Write about 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