Past-paper walk-through

Cyber security ▪ 5.3

eXercise

Questions in this set

- 0478/11 N25 Q4 ▪ 16 marks
- 0478/13 N25 Q4 ▪ 12 marks
- 0478/12 J24 Q8 ▪ 6 marks
- 0478/11 N23 Q6 ▪ 4 marks
- 0478/12 N23 Q1 ▪ 3 marks
- 0478/12 N23 Q8 ▪ 6 marks
- 0478/11 J23 Q8 ▪ 10 marks
- 0478/11 J23 Q10 ▪ 14 marks
- 0478/12 M23 Q1 ▪ 10 marks

Reading the mark scheme

- **B1** a mark that stands on its own – the point is either made or not.
- **M1** a *method* mark: the right approach, even if the number is wrong.
- **A1** an *answer* mark, and it usually needs its M mark first.
- **C1** a working mark on the way to the answer.
- // separates answers the examiner accepts equally.
- **ecf** = error carried forward: a later part is marked on your own earlier answer.
- **owtte** = "or words to that effect" – the wording need not match.

Question 4

0478/11 N25 ▪ Q4 ▪ 16 marks

A computer game development company are reviewing their current security solutions. The company wants employees to be aware of how they can identify phishing.

(a) Describe the process of phishing. **[4]**

Question 4

0478/11 N25 ▪ Q4 ▪ 16 marks

A computer game development company are reviewing their current security solutions.

The company wants employees to be aware of how they can identify phishing.

(b) Give **two** ways an employee could identify phishing.

1. 2. **[2]**

Question 4

0478/11 N25 ▪ Q4 ▪ 16 marks

A computer game development company are reviewing their current security solutions.

The company wants employees to be aware of how they can identify phishing.

(c) The company has installed anti-malware software on all employees' computers.

Give **three** examples of malware that anti-malware software can detect.

1. 2. 3. **[3]**

Question 4

0478/11 N25 ▪ Q4 ▪ 16 marks

A computer game development company are reviewing their current security solutions.

The company wants employees to be aware of how they can identify phishing.

(d)(i) State what is meant by a high-level language. **[1]**

(d)(ii) One benefit of using a high-level language is that the code is easy to debug.

Give **two** other benefits of using a high-level language.

1. 2. **[2]**

(d)(iii) One drawback of using a high-level language is that it must be converted to a low-level language before it can be run.

Give **one** other drawback of using a high-level language. **[1]**

(d)(iv) The computer game developers use an interpreter instead of a compiler when developing the computer game.

Question 4

Explain why an interpreter would be more appropriate for developing the computer game. **[3]**

Solution 4

(a)

Mark scheme

- Any four from:
- ▪ A legitimate looking email is sent to the user
- ▪ The user clicks a link in the email // the user replies to the email
- ▪ The user is directed to a fake website
- ▪ The user enters their personal data ...
- ▪ ... that is stolen/used by a third party (for malicious purposes)

Solution 4

(b)

Mark scheme

- Any two from:
- ▪ Check the email address that the email has been sent from
- ▪ Check the tone/spelling of the email
- ▪ Check the URL that is attached to the link

Solution 4

(c) Mark scheme

- Any three from:
- For example:
- ▪ Virus
- ▪ Worm
- ▪ Trojan horse
- ▪ Spyware // keylogger
- ▪ Ransomware
- ▪ Adware

Solution 4

(d)(i)

Mark scheme

- Any one from:
- ▪ A language that uses English-like statements
- ▪ It is a language that needs to be converted to machine code (to be processed by a computer)
- ▪ It is a portable language (that can be used on any computer)

Solution 4

(d)(ii)

Mark scheme

- Any two from:
- ▪ Easy/quick to read/write/understand
- ▪ Machine independent
- ▪ Less likely to make errors
- ▪ Programmer can focus on the problem instead of the manipulation of memory/hardware

Solution 4

(d)(iii)

Mark scheme

- Any one from:
- ▪ Cannot directly manipulate the hardware
- ▪ Takes longer to convert (than low level-language)
- ▪ Cannot use specialised hardware
- ▪ Uses more memory // less efficient memory use

Solution 4

(d)(iv) Mark scheme

- Any three from:
- ▪ The code is translated and executed line by line
- ▪ ... stopping when an error is found (showing the error location)
- ▪ ... meaning errors can be corrected in real time
- ▪ No need to retranslate each time an error is fixed
- ▪ ... making it easier to debug
- ▪ Sections of code can be easily tested
- ▪ ... meaning the whole program doesn't need to be written for testing

Question 4

0478/13 N25 ▪ Q4 ▪ 12 marks

A cyber security company specialises in security solutions that help prevent hackers being successful.

(a) Identify **two** security solutions that can be provided to help prevent hackers being successful.

Explain how each solution helps prevent hackers being successful.

Solution 1

Solution 2 **[6]**

(b) The company also has a web page that provides information to improve people's awareness of social engineering.

Describe what is meant by social engineering. Include an example of social engineering in your answer. **[3]**

(c)(i) State **one** similarity between session cookies and persistent cookies. **[1]**

Question 4

(c)(ii) Explain one difference between session cookies and persistent cookies. **[2]**

Solution 4

(a) Mark scheme

- One mark for the security solution
- Two marks for a matching description
- ▪ Strong/complex password
- ▪ Requires a mixture of letters, number and symbols
- ▪ Makes it very difficult for the hacker to guess
- ▪ Limiting number of attempts for password
- ▪ Cannot keep repeatedly guessing a password
- ▪ Stops a brute-force attack being successful

Solution 4

- ▪ Biometric device
- ▪ Requires the hacker to have biometric data to access the data
- ▪ It is very difficult to fake biometric data
- ▪ Two-step verification // two-factor authentication
- ▪ Requires the hacker to have additional data to access the data
- ▪ The data is sent to the users registered device/account that the hacker would also need
- ▪ Firewall
- ▪ Examines incoming data/traffic
- ▪ Can block any data that does not meet set criteria

Solution 4

- Anti-spyware
- Detects/removes any spyware present on the computer
- Hacker cannot use spyware to get data to discover passwords

Solution 4

(b) Mark scheme

- Two marks for:
- ▪ Involves manipulating/deceiving people
- ▪ ... with the aim of obtaining confidential/personal/valuable data
- Any one from:
- For example:
- ▪ Phishing // by example
- ▪ Baiting // by example
- ▪ Shoulder surfing // by example

Solution 4

(c)(i) Mark scheme

- Any one from:
- ▪ They are both small text files
- ▪ They both store data about the user // by example
- ▪ They are both stored/managed by the web browser
- ▪ They are both downloaded on to a user's computer
- 1
- October/November
- 2025

Solution 4

(c)(ii)

Mark scheme

- Two from (one mark for session, one mark for matching comparison to persistent):
- ▪ Session cookies are deleted when the web browser is closed
- ▪ ... whereas persistent cookies are deleted by the user/expire after a certain time
- ▪ Session cookies are only stored in RAM
- ▪ ... whereas persistent cookies are stored in the secondary storage

Question 8

0478/12 J24 ▪ Q8 ▪ 6 marks

A company has a website that is suffering a distributed denial of service (DDoS) attack.

(a) Draw and annotate a diagram to show the process of the DDoS. **[5]**

(b) Identify a solution that can be used to help prevent the DDoS attack being successful. **[1]**

Solution 8

(a) Worked steps

Draw the actors as labelled boxes — the **perpetrator**, the **infected computers (bots)**, and the **target server** — with annotated arrows between them. One mark for each correct part of the diagram.

- A **perpetrator sends malware** to many computers, or users download and install it.
- Those computers become a **botnet** of infected machines, under the attacker's control.
- The attacker **triggers them all at once** to send requests to the target.
- The **server is flooded** with more requests than it can handle …
- … so **legitimate users cannot access it** — the service is denied.

Solution 8

The word that has to be visible in the annotation is **distributed**: the requests come from **many** machines at once, which is what separates a DDoS from a plain DoS and what makes it hard to block by address.
State the **effect** as well as the mechanism. The last mark is for the consequence — the server slows or crashes and genuine users are refused — and a diagram that stops at "requests are sent" has not shown the attack succeeding.
Label the arrows with what travels along them: malware first, then the flood of requests. **Mark scheme**

- One mark for each part of the diagram that shows:
- ▪

Solution 8

- A perpetrator/third party sending malware // user downloads/installs malware
- ▪
- Each computer is turned into a bot...
- ▪
- ... to create a botnet
- ▪
- Third party initiates the attack
- ▪
- All the bots send a request at once to a web server
- ▪

Solution 8

- ... crashing the webserver
- Example:

Solution 8

(b) Mark scheme

- Proxy server
- 1 third party bot bot bot bot web server
- Third party sends malware.
- Malware turns computers into bots.
- Botnet
- Requests
- Web server cannot handle all the requests and crashes.

Question 6

0478/11 N23 ▪ Q6 ▪ 4 marks

6 Draw and annotate a diagram to demonstrate how a firewall works.
[4] **[4]**

Solution 6

Worked steps

Draw the firewall as a box **between** the internal network (or computer) and the internet, with traffic crossing it. Any four of the following, each annotated on the diagram:

- **Traffic passes both ways** through the firewall — incoming and outgoing.
- The firewall **examines each packet** against a set of criteria or rules.
- It **compares the traffic to a blacklist and a whitelist** of addresses.
- Traffic that **fails the criteria is blocked**; traffic that passes is allowed through.
- It **keeps a log** of traffic, which can be examined later.
- It can **warn the user** about an attempted intrusion.

Solution 6

Worked steps

The single most important feature of the drawing is the **position**: the firewall sits on the boundary, so every line between inside and outside passes through it. A firewall drawn beside the network rather than across the link has missed what it does.
Both directions is a mark of its own, and it is the one most often lost. A firewall filters what leaves as well as what arrives — which is how it stops software on an infected machine from calling out.
Annotate the arrows with what is being checked and what happens to it. The marks are for the described behaviour, not for the box. **Mark scheme**

- The diagram includes (any four from):
- —

Solution 6

Worked steps

- Traffic passing both ways through the firewall
- –
- An indication that criteria is set for the firewall
- –
- Traffic is compared to criteria
- –
- Traffic being rejected if it does/does not meet criteria
- –
- Traffic being accepted if it does/does not meet criteria

Solution 6

Worked steps

- e.g.
- 4

Question 1

0478/12 N23 ▪ Q1 ▪ 3 marks

1 Malware can be used to corrupt data stored on a computer.

(a) Tick (✓) **one** box to show which cyber security threat is **not** a type of malware.

A	Phishing	☐
B	Ransomware	☐
C	Virus	☐
D	Worm	☐

[1]

(b) Identify **one** other example of malware than those given in **part 1(a)**.

Question 1

(c) Identify the type of software that is used to find and remove malware from a computer.

Solution 1

(a)

Mark scheme

- —
- A
- 1

Solution 1

(b) Mark scheme

- Any one from:
- –
- Spyware // Keylogger
- –
- Adware
- –
- Trojan horse
- 1

Solution 1

(c)

Mark scheme

- —
- Anti-malware
- 1

Question 8

0478/12 N23 ▪ Q8 ▪ 6 marks

8 **(a)** Draw and annotate a diagram that demonstrates the cyber security threat of data interception.

Question 8

[4]

(b) Identify **one** security solution that will help keep data safe from data interception and state why it will help keep the data safe.

Solution 8

(a) Mark scheme

- The diagram demonstrates (One mark for each part of the diagram):
- –
- Data is being sent from one device to another
- –
- The data is being examined during transmission
- –
- Packet sniffer is used
- –

Solution 8

- Intercepted data is reported to a third-party during transmission ...
- —
- ... and analysed for anything useful
- —
- Connection hacked to spoof destination address
- e.g.
- 4

Solution 8

(b) Mark scheme

- –
- Encryption ...
- –
- ... if the data is intercepted it will be meaningless (because they do not
- have the decryption key)
- 2
- 0478/12
- October/November

Solution 8

- 2023

Question 8

0478/11 J23 ▪ Q8 ▪ 10 marks

8 A manager at a company is concerned about a brute-force attack on its employee user accounts.

(a) Describe how a brute-force attack can be used to gain access to the employee user accounts.

Question 8

(b) One possible aim for carrying out a brute-force attack is to install malware onto the company network.

(i) State **two** other aims for carrying out a brute-force attack to gain access to the employee user accounts.

Question 8

[2]

(ii) Identify **three** types of malware that could be installed.

Question 8

[3]

(c) Give **two** security solutions that could be used to help prevent a brute-force attack being successful.

Question 8

[2]

Solution 8

(a) Mark scheme

- Three from:
- ▪
- Trial and error to guess a password
- ▪
- Combinations are repeatedly entered ...
- ▪
- ... until correct password is found
- ▪

Solution 8

- Can be carried out manually or automatically by software
- 3

Solution 8

(b)(i) Mark scheme

- Any two from:
- e.g.
- ▪
- Steal/view/access data
- ▪
- Delete data
- ▪
- Change data

Solution 8

- ▪
- Lock account // Encrypt data
- ▪
- Damage reputation of a business
- 2
- 0478/11
- May/June 2023

Solution 8

(b)(ii) Mark scheme

- Any three from:
- e.g.
- ▪
- Virus
- ▪
- Worm
- ▪
- Trojan horse

Solution 8

- ▪
- Spyware
- ▪
- Adware
- ▪
- Ransomware
- 3

Solution 8

(c) Mark scheme

- Any two from:
- ▪
- Two-step verification//Two-factor authentication//by example
- ▪
- Biometrics
- ▪
- Firewall // Proxy-server
- ▪

Solution 8

- Strong/complex password // by example
- ▪
- Setting a limit for login attempts
- ▪
- Drop-down boxes
- ▪
- Request for partial entry of password
- 2

Question 10

0478/11 J23 ▪ Q10 ▪ 14 marks

10 A student uses the internet for their schoolwork to research what is meant by pharming.

(a) State the aim of pharming.

Question 10

(b) Draw and annotate a diagram to represent the process of pharming.

Question 10

[4]

(c) The student uses a web browser to access data on the internet.

Explain the purpose of the web browser.

Question 10

(d) Storing cookies is one function of the web browser.

Give **three** other functions of the web browser.

Question 10

[3]

(e) A student visits a website that uses session cookies, instead of persistent cookies.

Explain the difference between session cookies and persistent cookies.

Solution 10

(a)

Mark scheme

- ▪
- To obtain personal data/details // by example
- 1

Solution 10

(b) Mark scheme

- One mark for each correct part of the diagram.
- Diagram shows:
- ▪
- User clicks/opens attachment/link that triggers download
- ▪
- Malicious software downloaded onto user's computer
- ▪
- User enters website address

Solution 10

- ▪
- User is redirected to fake website
- e.g.
- 4
- User
- computer
- Real
- website
- Fake
- website

Solution 10

- User clicks link that
- downloads malware
- to computer
- User types in
- web address
- Request
- gets
- redirected
- malware
- 0478/11

Solution 10

- May/June 2023

Solution 10

(c)

Mark scheme

- Two from:
- Displays web pages
- ... by rendering HTML
- 2

Solution 10

(d) Mark scheme

- Any three from:
- e.g.
- ▪
- Storing bookmarks/favourites
- ▪
- Recording user history
- ▪
- Allowing use of multiple tabs

Solution 10

- ▪
- Providing navigation tools // by example
- ▪
- Providing an address bar
- ▪
- Managing protocols // by example // checking digital certificate
- ▪
- Send URL to DNS
- ▪

Solution 10

- Sends a request to the IP address/web server (to obtain the contents of a webpage)
- ▪
- Runs active script/JavaScript/client-side script
- ▪
- Allows files to be downloaded from website/internet
- 3

Solution 10

(e) Mark scheme

- Any four from:
- ▪
- Session cookies are stored in memory/RAM
- ▪
- ... whereas persistent cookies are stored on the hard drive/secondary storage
- ▪
- When the browser is closed a session cookie is lost
- ▪

Solution 10

- ... whereas a persistent cookie is not lost
- ▪
- ... until deleted by the user/they expire
- 4

Question 1

0478/12 M23 ▪ Q1 ▪ 10 marks

1 Computers can be infected with malware. Spyware is one example of malware.

(a) Tick (✓) **one** box to show a correct definition of spyware.

A Software that activates a webcam and transmits the video to a third party that outputs it live on a website. ☐

B Software that detects when a password is being entered and then emails the password to a third party. ☐

C Software that records all data entered into a computer, analyses this data to find email addresses and passwords, then posts these to a website. ☐

Question 1

D Software that records all key presses and transmits these to a third party. ☐

[1]

(b) Complete the table by identifying and describing **two** other examples of malware.

	Malware	Description
1	.....	.....
	.....	.....

Question 1

		.....
2	....	....

[6]

(c) Proxy-servers and firewalls have some similar functions.

Question 1

Identify **two** similarities and **one** difference between proxy-servers and firewalls.

Question 1

[3]

Solution 1

(a)

Mark scheme

- D
- 1

Solution 1

(b) Mark scheme

- One mark for identification. E.g. One mark per bullet for description to max
- two each.
- Virus
- ▪
- Software/code that replicates
- ▪
- ...when the user runs it // with an active host
- ▪

Solution 1

- Deletes/damages/corrupts data/files // takes up storage/memory space
- Worm
- ▪
- Software/code that replicates itself on a network
- ▪
- ...without user input // without active host
- ▪
- Takes-up bandwidth
- ▪
- Deletes/damages/corrupts data/files // takes up storage/memory space

Solution 1

- ▪
- Opens back doors to computers over the network
- ▪
- Used to deposit other malware on networked computers
- Trojan horse
- ▪
- Software/code that is hidden within other software // Software that is
- disguised as authentic software
- ▪
- ...when downloaded/installed the other malware/by example it

Solution 1

- contains is installed
- Adware
- ▪
- Software/code that generates/displays (unwanted) adverts on a user's
- computer
- ▪
- Some may contain spyware/other malware
- ▪
- Some when clicked may link to viruses
- ▪

Solution 1

- Reduces device performance // reduces internet speed
- ▪
- Redirects internet searches/user to fake websites
- Ransomware
- ▪
- Software/code that stops a user accessing/using their computer/data
- ▪
- ...by encrypting the data/files/computer
- ▪
- A fee has to be paid to decrypt the data // A fee has to be paid to

Solution 1

- 'release' the computer/device/data
- 6
- 0478/12
- February/March 2023

Solution 1

(c) Mark scheme

- One mark for each similarity to max two. One mark for difference (both
- sides needed unless clearly and accurately implied).
- Similarities e.g.
- ▪
- Check incoming and outgoing signals // filter traffic
- ▪
- Store whitelist/blacklist
- ▪

Solution 1

- Block incoming/outgoing signals
- ▪
- Both block unauthorised access
- ▪
- Keep a log of traffic
- ▪
- Both can be hardware or software (or both)
- Differences e.g.
- ▪
- Proxy can hide user's IP address, firewall does not hide the user's IP

Solution 1

- address
- ▪
- Proxy intention is to divert attack from server, firewall is to stop
- unauthorised access
- ▪
- Proxy protects a server, firewall protects individual computer
- ▪
- Proxy examines/processes requests for a website but a firewall does
- not (checks type of signal) // Proxy processes client-side requests
- whereas firewall filters packets

Solution 1

- ▪
- Proxy transmits website data to the user, but a firewall does not (it
- allows valid signals)
- ▪
- Proxy allows faster access to a web page using cache, but a firewall
- does not (allow faster access or have cache)
- ▪
- Proxy can hide internal network from internet, but a firewall cannot
- 3
- 0478/12

Solution 1

- February/March 2023