LEVEL 3 TECHNICAL LEVEL
IT: Networking

A/507/6495 – Unit 6: Network Security Management

Mark scheme

June 2018

Version/Stage: 1.0 Final

Mark schemes are prepared by the Lead Assessment Writer and considered, together with the relevant questions, by a panel of subject teachers. This mark scheme includes any amendments made at the standardisation events which all associates participate in and is the scheme which was used by them in this examination. The standardisation process ensures that the mark scheme covers the students' responses to questions and that every associate understands and applies it in the same correct way. As preparation for standardisation each associate analyses a number of students' scripts. Alternative answers not already covered by the mark scheme are discussed and legislated for. If, after the standardisation process, associates encounter unusual answers which have not been raised they are required to refer these to the Lead Assessment Writer.

It must be stressed that a mark scheme is a working document, in many cases further developed and expanded on the basis of students' reactions to a particular paper. Assumptions about future mark schemes on the basis of one year's document should be avoided; whilst the guiding principles of assessment remain constant, details will change, depending on the content of a particular examination paper.

Further copies of this mark scheme are available from aqa.org.uk

The following annotation is used in the mark scheme:

; - means a single mark

// - means alternative response

/ - means an alternative word or sub-phrase

A - means acceptable creditworthy answer

R - means reject answer as not creditworthy

NE - means not enough

I - means ignore

DPT - in some questions a specific error made by a candidate, if repeated, could result in the candidate failing to gain more than one mark. The DPT label indicates that this mistake should only result in a candidate losing one mark on the first occasion that the error is made. Provided that the answer remains understandable, subsequent marks should be awarded as if the error was not being repeated.

Level of response marking instructions

Level of response mark schemes are broken down into levels, each of which has a descriptor. The descriptor for the level shows the average performance for the level. There are marks in each level.

Before you apply the mark scheme to a student's answer read through the answer and annotate it (as instructed) to show the qualities that are being looked for. You can then apply the mark scheme.

Step 1 Determine a level

Start at the lowest level of the mark scheme and use it as a ladder to see whether the answer meets the descriptor for that level. The descriptor for the level indicates the different qualities that might be seen in the student's answer for that level. If it meets the lowest level then go to the next one and decide if it meets this level, and so on, until you have a match between the level descriptor and the answer. With practice and familiarity you will find that for better answers you will be able to quickly skip through the lower levels of the mark scheme.

When assigning a level you should look at the overall quality of the answer and not look to pick holes in small and specific parts of the answer where the student has not performed quite as well as the rest. If the answer covers different aspects of different levels of the mark scheme you should use a best fit approach for defining the level and then use the variability of the response to help decide the mark within the level, ie if the response is predominantly level 3 with a small amount of level 4 material it would be placed in level 3 but be awarded a mark near the top of the level because of the level 4 content.

Step 2 Determine a mark

Once you have assigned a level you need to decide on the mark. The descriptors on how to allocate marks can help with this. The exemplar materials used during standardisation will help. There will be an answer in the standardising materials which will correspond with each level of the mark scheme. This answer will have been awarded a mark by the Lead Examiner. You can compare the student's answer with the example to determine if it is the same standard, better or worse than the example. You can then use this to allocate a mark for the answer based on the Lead Examiner's mark on the example.

You may well need to read back through the answer as you apply the mark scheme to clarify points and assure yourself that the level and the mark are appropriate.

Indicative content in the mark scheme is provided as a guide for examiners. It is not intended to be exhaustive and you must credit other valid points. Students do not have to cover all of the points mentioned in the Indicative content to reach the highest level of the mark scheme.

An answer which contains nothing of relevance to the question must be awarded no marks.

Question	Guidance	Mark
01	C	1
02	A	1
03	D	1
04	B	1
05	B	1

Question	Guidance	Mark
06	**1 mark** (max **2 marks**) for each point or expansion point, eg: • never be able to keep up with and catch all the vulnerabilities manually • to identify new threats // attacks can take place at any time / regularly • threat can be dealt with immediately // instant notification • new vulnerabilities become known / were not previously exploitable • cheaper than employing staff to do this, even if they could • cloud-based options now provide scanning.	**2**
07	**1 mark** (max **2 marks**) for each point or expansion point, eg: • email attachments are often unsolicited / from unknown senders • email may contain links to malicious web sites / contain malicious software; such as a jpeg; • a downloaded file may be a malicious application; such as a Trojan; • example of the potential harm / consequence. **A.** counter point (max **1 mark**), eg: • keeping anti-virus installed / up to date is the best defence // scan files before opening them • attachment may be stored on hard drive whether opened or not • email client / network policies might prevent / block attachments.	**2**
08	**Threat:** **1 mark** for any of the following, eg: • unauthorised access point • compares / identifies (non-approved) MAC addresses • identifies any not known / not approved frequencies / spectrum • unauthorised user / device / AP • man-in-the-middle attack • honeypot attack • denial-of-service attack // flood of requests / data • injection attack. **A.** IP address instead of MAC address **R.** intrusion / intrusion detection // malicious activity. **Response:** **1 mark** for any of the following, eg: • WIPS server classifies / validates threat and notifies administrator • blocks wireless devices generating unknown / unapproved frequencies • it could block it. **A.** any reference to: logging / recording / receiving information, provided there is also some reference to logging / recording / receiving information on a (WIPS) server.	**2**

Question	Guidance	Mark
09	**1 mark** (max **2 marks**) for any of the following, eg: • denying access to Internet / intranet / revoking authorised user status • fine or payment of compensation for misuse of resources • disciplinary process up to and including removal, dismissal, or exclusion • prosecution according to law.	**2**
10.1	**1 mark** for appropriate reference to any of the following, eg: • rules and procedures governing communication over a network • rules and procedures intended to make communication between two or more devices over a network possible. **A.** rules / procedures // a set of rules / procedures. **R.** instructions // a set of instructions // regulations.	**1**
10.2	**1 mark** (max **2 marks**) for any of the following, eg: • more sophisticated / better data encryption • enhanced user authentication // WEP's user authentication considered inadequate • it is more secure // the transmissions are more secure • it allows for a longer password (which is theoretically more secure) • 256-bit keys (instead of 40/64/128 bit) • addressed initialisation vector issue • message integrity checks / TKIP. **A.** increased bits for encryption.	**2**

Question	Guidance	Mark
11	**1 mark** for any reference to: • two-factor authentication // 2FA // multi-factor authentication // two-step verification // TFA • tokenless authentication • biometrics, eg iPhone fingerprint / facial recognition • a selection of characters from a password / phrase (not the whole phrase). **1 mark** (max **2 marks**) for each point or expansion point: • hardware-based, user-authentication // connected tokens • generate codes, passcodes, secondary log-in prompts // disconnected tokens • security token // authentication token // hardware token // one-time password authentication // OTP • security / encrypted key / signature • app passwords // app verification codes // PINsentry • two pieces of evidence • information (only) the user has or has immediately to hand • two-step verification helps prevent a brute force attack • nobody (in theory) has the same biometric reading.	**3**
12.1	**1 mark** (max **3 marks**) for each example, eg: • Where is critical or sensitive information stored or processed? • Where is business-critical or high value equipment / material located (and whether onsite or offsite)? / Place server in a safe area. • What impact would the loss of each business-critical asset / activity have on business-critical functions, operations, or users / customers? • provide training for end users and administrators • making information available only to authorised entities • operational security / access control // privileges // user data / profile of users • physical security / (existing) hardware / software • security & control / (review of) security & control threats / countering security & control threats • communications security / tapping & spoofing • procedural security / software installation & administration • firewalls / security tools	**3**
12.2	**1 mark** (max **3 marks**) for each issue, eg: • Is a vulnerability better minimised using physical or IT measures? / What are the vulnerabilities? • Do the costs of enhanced resources necessary to secure an asset exceed the value of the asset / its importance / sensitivity of data? • Is a countermeasure effective across the system / within specific areas? // How risks are mitigated. • Do current plans suggest a vulnerability is likely to become irrelevant? • How long will it take to fully implement all proposed enhancements? • issues to prioritise, eg not leaving most vulnerable to last • any reference to “impact” / business contingency planning if not already referenced in the candidate’s response in 12.1.	**3**

	A. Operating system level issue, eg whether to allow USB access. **A.** Procedural level issue, eg assessment of employee risk / access rights. **A.** Physical level, eg access to a server room or network cables.	
Question	**Guidance**	**Mark**
13	**1 mark** (max **3 marks**) for each point or expansion point, eg: • someone who (legitimately) attempts to penetrate a system or network / determine its weaknesses and vulnerabilities • uses same tools as malicious hacker but in lawful / legitimate manner • identifies vulnerabilities a malicious hacker could exploit • ethical "white hat" hacker v malicious "black hat" hacker • determines how to minimise risk // improve overall security // assess the security posture • weaknesses identified or tested be physical or human, hardware or software related • an example of penetration testing (eg intrusion testing, red teaming).	**3**
14.1	**1 mark** (max **2 marks**) for each item, eg: • user activity, eg IDs / access rights • date and time of log on and log off, other key events • successful and failed attempts to access systems / data / applications • files / data accessed / modified • files and folders (eg for integrity) • use of system utilities • web activity // network traffic • a router / modem / switch • incoming connections • data packets / packet log • event log • downloads • MAC addresses • IP addresses.	**2**
14.2	**1 mark** (max **2 marks**) for any of the following, eg: • troubleshooting issues • investigating security incidents / unusual activity • alerts / awareness / prevention • provide audit trails when investigating an incident. **What might cause concern or need further investigation?** **1 mark** (max **2 marks**) for any of the following, eg: • security-related events, eg alarms triggered / alerts / IDS • individual activity beyond accepted tolerances / access rights • activity outside baselines of what is expected / acceptable • files missing / failed integrity checks.	**4**

Question	Guidance	Mark
15	**1 mark** (max 3 marks) each criterion plus **1 mark** for each expansion point, eg: • anti-virus scanning: full scan at least once daily; performance determined by number of daily full scans completed in working week; • anti-virus software updates: up and running within 1 hour of availability; performance determined by number of computers using updated software within 1 hour; • virus / worm attacks: isolated, neutralised within 1 hour of being identified; performance determined by number of computers available and accessible within 1/3/5 hours (dependent on severity); • unpatched / unmanaged machines, CNSM: managed systems are ALWAYS up to date and available (OS and Apps); performance determined by number of managed machines unexpectedly unavailable or not up to date; • critical updates, vulnerabilities; performance measures; • service hours / times during which network is monitored / response is available. **R.** Similar expansion points.	**6**
16	**1 mark** (max **4 marks**) for any of the following, eg: • a packet sniffer looks at / scans / examines / analyses each packet; this can be used to retrieve / steal (unencrypted) data; such as passwords; • packets are captured / intercepted; stored / logged; and (later) decoded / examined; • a packet is part of a message that is broken up // networks move data around in small packets • a packet sniffer monitors traffic conversations // can see all the information passing over the network it is connected to; any data which is not encrypted is readable; • might generate auto-response, eg flag administrator • (used maliciously) to detect data / vulnerabilities which can be exploited • each packet carries the information needed to get to its destination • information carried includes the sender's IP address // receiver's IP address; packet sniffers are therefore very useful to hackers. Example 4-mark answer: A packet sniffer monitors network traffic; packets are captured; and stored; so they can be decoded later;	**4**

Question	Guidance	Mark
17	**Front end security:** **1 mark** (max **3 marks**) for each point, eg: • the design and implementation phase • the first line of defence // perimeter security • categorising information systems • selecting security controls • implementing security controls. **A.** discover, classify, apply. **A.** examples, eg firewall. **Back end security**: **1 mark** (max **3 marks**) for each point, eg: • finalising audits • assessing security controls • authorising information systems • continuous monitoring / improving of security controls. **A.** analyse, action, monitor.	**6**

Question	Guidance	Mark
18.1	**1 mark** (max **4 marks**) for each form of abuse, eg: • phishing // spear fishing • adware • spyware • spam • (unauthorised) hacking into email account. **R.** pharming.	**4**
18.2	**1 mark** (max **2 marks**) for each example, **1 mark** for each expansion point, eg: • email identified as having a virus; nevertheless released by employee; • virus contained within an email; which could not be analysed by filtering system; • deliberate / malicious (self) infection of system by employee; • encrypted email / password protected file; • the security issue has been specifically caused by the client // client has white-listed harmful email; • client / employee fails to report a known issue; **A.** when the terms and conditions have not been met.	**4**
19	**1 mark** (max **3 marks**) for each offence, eg: • HACKING / unauthorised access to computer material from outside organisation / unauthorised access internal to organisation • UNAUTHORISED MODIFICATION of computer material / any reference to fraud or intellectual property rights • UNAUTHORISED ACCESS / any reference to intent to commit further offences. • UNAUTHORISED ACTS / any reference to intent to impair; causing, or creating risk of, serious damage; • making, supplying or obtaining articles for use in the above. **1 mark** (max **4 marks**) for acceptable indication as to why some offences attract more severe penalties than others, eg: • potential to cause more damage, eg: accessing a computer less damaging than modifying computer material • type of installation hacked, eg accessing a military computer more serious than accessing a home computer • planning / premeditation / intent.	**7**

<table>
<tr><th>Question</th><th>Guidance</th><th>Mark</th></tr>
<tr><td>20</td><td>
1 mark (max 5 marks per row) for each element of any of the following:

A. other valid points (for any column).

<table>
<tr><th></th><th>DEFINE
(2 marks)</th><th>EXAMPLE
(1 mark)</th><th>EXPLAIN
(2 marks)</th></tr>
<tr><td>AUTHENTICATION</td><td>Credentials of user compared with those stored on file; process of verifying who you are</td><td>PASSWORD

CAPTIVE PORTAL</td><td>restricts access to network / to approved users only</td></tr>
<tr><td>AUTHORISATION</td><td>Specifying access rights / privileges / what you’re allowed to do as defined in access policy; process of verifying access</td><td>AUTHORISATION CHECKS

PERMISSIONS

A. ADMIN PASSWORD</td><td>protects data on system by restricting access to authorised users only</td></tr>
<tr><td>ACCESS CONTROL</td><td>Uses both authentication and authorisation to control user access</td><td>LOCKS
LOGINS
ROLE-BASED

CAPTIVE PORTAL (eg bypass for approved devices)</td><td>user granted to only what they need to access / an individual could view their own details but not, for example, view or change those of others - but their manager might well have those higher privileges to allow change</td></tr>
</table>
</td><td>15</td></tr>
</table>

Assessment Outcomes					
Question	**AO1**	**AO2**	**AO3**	**AO4**	**Question Total**
Section A					
1				4a (1)	**1**
2	1d (1)				**1**
3	1c (1)				**1**
4				4c (1)	**1**
5		2d (1)			**1**
6			3c (2)		**2**
7		2e (2)			**2**
8			3a (2)		**2**
9				4a (2)	**2**
10.1		2b (1)			**1**
10.2		2d (2)			**2**
11	1a (3)				**3**
12.1				4c (3)	**3**
12.2	1b (3)				**3**
13	1b (3)				**3**
14.1			3b (2)		**2**
14.2			3b (4)		**4**
15				4b (6)	**6**
16			3c (4)		**4**
17			3a (6)		**6**
Section B					
18.1				4b (4)	**4**
18.2				4b (4)	**4**

19	1d (7)				**7**
20	1bc (6)	2abc (9)			**15**
Total	**24**	**15**	**20**	**21**	**80**