Level 3 Technical Level
IT: NETWORKING
A/507/6495

Unit 6 Network security management

Mark scheme
January 2018

Version: 1.0 Final

181AA5076495/MS

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

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
1	D	**1**
2	A	**1**
3	C	**1**
4	A	**1**
5	D	**1**
6	**State one way in which a denial-of-service attack (DoS attack) is different from a distributed denial-of-service attack (DDoS attack).** **1 mark (max 1 mark)** for explanation, eg • **DoS** attack typically uses one computer and one Internet connection to flood a targeted system or resource. • **DDoS** attack uses multiple computers and Internet connections to flood the targeted resource / ACCEPT "larger scale attack"	**1**
7	**Malware is an abbreviation meaning ‘malicious software’. Both spyware and adware are forms of malware. Explain why spyware may have more serious consequences adware.** **1 mark (max 2 marks)** for • **Spyware** obtains covert information about another's computer activities • by transmitting data (covertly) from their hard drive • **Adware** displays or downloads advertising material such as banners or pop-ups when a user is online • annoying but harmless, unwanted but can be ignored	**2**
8	**Explain why spear phishing attacks are far more likely to succeed than traditional phishing attacks.** **1 mark** for any of the following **(max 2 marks)** • selective, targeted, personalised, tailored, focussed(ACCEPT anything similar) • e-scamming, deceptive, fraudulent, impersonation, spoof email, look alike domains • tricking/prompting/persuading victims into performing actions/exploiting vulnerabilities	**2**

9	**State two security improvements WPA2 provides compared with WPA.** **1 mark** for any of the following **(max 2 marks)** • Use of (AES) algorithms • Use of CCMP (Counter Cipher Mode protocol) • (far more) random encryption keys , ACCEPT "larger encryption key", "better encryption" Award max 2 marks if detail in brackets provided.	**2**
10.1	**Give another example of perimeter security.** **1 mark** for any of the following **(max 1 mark)** • Intrusion Detection and Prevention Systems (ACCEPT IDS/IDPS) • Antivirus and Anti-Spam, Malware detection • Honeypots • Virtual private network (VPN) encryption • Web filtering • Scanning inbound and outbound user traffic / looking for suspicious patterns • Demilitarised Zone (ACCEPT DMZ) ACCEPT "routers"	**1**
10.2	**Even if your client's perimeter systems are fully up to date, new attacks will still get through. Using the layered-security model, give one example of added protection under each of the following headings:** **Network** **1 mark** (max. 1 mark) for an example, eg • Intrusion detection system (IDS) • Intrusion prevention system (IPS) • Vulnerability management system • Network access control • (Network) User authentication **Host** **1 mark** (max. 1 mark) for an example (**not** repeating a response already given above), eg • (Host) IDS • (Host) vulnerability assessment • (Network) access control • Antivirus • Host Access control • (Host) User authentication • Application shield • Application access control • (Access) User authentication • Input validation	**3**

	Data **1 mark** (max. 1 mark) for an example (**not** repeating a response already given above), eg • Encryption • Data access control • (Data) User authentication	

11	**List four examples of access control.** **1 mark (max 4 marks)** for each example, eg • Biometrics • Passwords • User permissions ACCEPT "User accounts, User privileges, Admin privileges" • Digital signatures, Special key • Protocols • Logins NOT "File permissions"	**4**

12	**For each phase describe one activity you might complete and what you would hope to achieve in doing so.** **Plan** **1 mark** for any **one** of the following, **1 mark** for a suitable expansion: • discover, classify, define policies, apply security measures / up to date audit intelligence, selecting and implementing security controls. **Monitor** **1 mark** for any **one** of the following, **1 mark** for a suitable expansion: • analyse, collect, aggregate / review, better understand how security measures are performing, defining risks (threats and vulnerabilities). **Action** **1 mark** for any **one** of the following, **1 mark** for a suitable expansion: • escalate, validate / finalising audits, improving controls, revising policy, scoping and implementing controls.	**6**

13.1	**Provide an example or explanation of what might be included for each of the four elements listed below.** **1 mark (max 2 marks)** for each element, eg • Responsibilities / who does what and by when / security and access • Expectations / guarantee of level of work demanded and timeframe within which any action will be taken, baseline compliance, performance and availability, agreed schedule. • Penalties / financial penalties for service failure, management within agreed budget, non-compliance, accidental damage, replacement cost • Incentives / measuring & rewarding success, exceeding expectations. **1 mark (max 2 marks)** for each suitable expansion.	**4**

13.2	**Give two potential benefits of a business having a service level agreement.** **1 mark** for any of the following **(max 2 marks)** • improves customer service / sets standards for customer service • identifies communication / escalation points • ensures customer expectations known / clear / all concerned know and understand what is expected of them • defines procedures (service groups and employees) • creates trust between client and provider • encourages customer loyalty • promotes return business / more business	**2**

14.1	**Explain how MAC association and the DHCP server can work together to better secure a network.** **1 mark** for any of the following **(max 2 marks)** • the DHCP server issues an IP address only if MAC address recognised • approved MAC addresses are populated by administrator • ALLOW "determines which devices are allowed access (to Network)" ACCEPT • any reference to "authorised listing" or "authorised / authorises (IP) addresses	**2**

14.2	**Explain why it is important to change SSID default settings.** **1 mark** for any of the following **(max 2 marks)** • using the default SSID risks another nearby network having the same name • a wi-fi device may auto-connect to any network with the same name • if wireless security options not enabled, anyone can connect to the network by knowing only the SSID	**2**

14.3	**Give one advantage of using symmetric encryption (rather than asymmetric encryption) and one security challenge inevitable when using symmetric encryption.** **1 mark** for advantage, eg • only uses one key, therefore faster, less complicated **1 mark** for challenge, eg • uses identical key to both encrypt and decrypt data • distributing shared key presents major security risk ALLOW "man-in-the-middle attack"	**2**

15	**Banner grabbing and port scanning are two network monitoring tools. For both network monitoring tools identify:** • **the information it can provide (1 mark)** • **how a hacker might exploit this tool (1 mark)** • **what counter-measures you might apply (1 mark)** **Banner grabbing** provides information about a computer system on a network and the services running on its open ports; can be used to take inventory of the systems and services on the network, can target IP address. **Hackers** can exploit this tool as identifies the operating system, version number, and service packs. **Counter** by disable default banners on network host or remove information from customisable banners. **(max 3 marks)** **Port scanning** provides information about available services running on a server or host; identifies open ports. **Hackers** can exploit this tool as identifies the operating system and if a firewall has been enabled; as a port is a place where information comes into and out of a computer, port scanning effectively identifies an open door. **Counter** by using port scanning to identify unauthorised hosts or applications or network host configuration errors, be thorough, perform same test on different utilities and compare results, blocking ports with a firewall ALLOW "disabling ports not in use". **(max 3 marks)**	**6**

16	**Explain how you would monitor a network system open to all (employees and visitors, with both desk bound access and remote access) ensuring security is maintained at all times.** From any **three** of the following: **1 mark** (max. 3 marks) for stating the business critical element **1 mark** (max. 3 marks) for a suitable expansion point • User accounts, unique accounts, no shared accounts, • Separation between normal user and privileged user accounts, VLANs • Credentials, multifactor authentication, routing protocols, 802.1X EAP • Review roles, access privileges, local group memberships set, privileges assigned • Disable stale accounts, delete really old ones • Vulnerability scan, add to regularly scheduled scans, weekly externals, monthly internals • Assigned workstations, network hardware list, network configuration, disabled ports • Logging and alerts • Local encryption, WPA • Backup, tape rotation, off-site storage, verify restores monthly, restricted access to tapes • Malware scanning, outbound traffic port blocking ALLOW "IPSec"	**6**

17.1

Give two benefits of allowing employees to BYOD and explain why network managers accommodate this risk.

1 mark (max 2 marks) for each benefit, eg

- improved employee job satisfaction
- increased employee job efficiency and flexibility
- cost savings on device purchase

1 mark (max 2 marks) for each explanation (different to the above), eg

- IT self-sufficiency now common among employees
- (their) mobile devices are often newer / more advanced
- saving on training, etc

4

17.2

Discuss the security challenges in having a BYOD environment.

Using the levels of response tables on following pages, award up to:
8 marks for security challenges

Indicative content:

- Employee owns, maintains, supports own device – risk to company is due to less control over device and loss of control of company data; where and how it is stored / data leakage; what happens to that data once employee leaves premises, ceases employment, etc
- (Noncompliant) device access without permission or protection; mixing business and personal; use of personal apps in a business environment; use of *insecure* content in a secure environment; jail-breaking / rooting of smartphones; family members access to same device, protected access to work data, control and restrictions; use of public cloud storage and public file sharing
- Absence of developed / established policy or effective monitoring to ensure most vulnerable devices (smartphones, tablets accessing Wi-Fi networks with few appropriate security protocols) have restricted / limited / no access to more sensitive data;
- Loss and theft; loss of data should employee leave, (mobile) device be lost, etc

Band	Descriptor	Identified	Discussed	Clearly understood
3	3 or 4 security challenges identified and discussed, with clear understanding	3	4-6	7-8
2	2 or more security challenges identified, with some discussion, and some understanding	2	3-4	5-6
1	1 or 2 security challenges identified, with some discussion but limited understanding	1	2-3	4

8

17.3

As Network Manager of a BYOD environment, explain how you would ensure secure network access for all BYOD users – not just permanent employees, but temporary staff, visitors and contractors alike.

Using the levels of response tables on following pages, award up to:
8 marks for methods of providing secure access

Indicative content:

- Policy predates technology, specifying what mobile devices will be supported and what will not; what software / apps may be accessed and what may not; data can be processed and what will not, what anti-malware is required and what is not
- What (type of) data is held, where that data can be stored, how and when it can be transferred or shared; avoidance of 'man-in-the-middle' attacks; more secure transfer options offered by, for example, a VPN acting like a gatekeeper, verifying data being transferred with encryption and permissions
- Specifying / prescribing named Operating Systems and Third Party Software; proscribing untrusted and non-verified market places / apps
- Audit data processed by user, by device; define, by user, who is allowed access to what data and to authorised / named devices only; **all** occasional (BYOD) users read and sign Acceptable Use Policy, likely to include reference to appropriate use / non-use of Social Media, processing / non-processing of personal data / exclusion of PII (personally identifiable information), call history, voice calls, etc
- prohibitions on public cloud storage, public back up services, etc
- Protocols for ensuring device summary data held does not become out of date or inaccurate over time
- □ □ Identify data that cannot be processed using (any) personal device and which can only be processed using more secure / restrictive / business equipment; BYOD must never introduce vulnerabilities into otherwise secure environments
- Business and personal use; clear separation; protocols for securing / limiting business access away from business premises; avoidance of disclosure of personal data should device have automated backup facility
- Protection from unauthorised or unlawful access should (mobile) device be lost or stolen (eg PIN, passwords, encryption, biometrics); agreed protocols for immediately revoking access should device be lost or stolen
- Specify storage allowable on any personal device, dependent on nature of data, commercial sensitivity may preclude removable memory cards, USB sticks, etc; may need to specify sandbox or ring-fence storage options for some data
- (Ensure pre-registration for) use of Mobile Device Management to delete remotely and / or on demand, geo-locate, etc

Band	Descriptor	Identified	Discussed	Clearly understood
3	3 or 4 controls identified and discussed, with clear understanding	3	4-6	7-8
2	2 or more controls identified, with some discussion, and some understanding	2	3-4	5-6
1	1 or 2 controls identified, with some discussion but limited understanding	1	2-3	4

17.4

Given the risks of BYOD to data control, list four things that a BYOD policy might include.

1 mark (max. 4 marks) for each point, eg

- Expectations / how to manage own device
- Devices to be included
- Device inspection / approval / audit
- What type of data is held
- Where data is stored
- How data is transferred
- Potential for / avoidance of data leakage / security / confidentiality
- Blurring of personal and business use
- The device's security capabilities
- What to do if the person leaves the business
- How to deal with loss, theft, failure, support of the device
- Compliance with business policy, protocols, etc
- Authentication and Access Control

4

17.5

The UK Information Commissioner's Office (ICO) has published BYOD guidance for employers on how to comply with the UK Data Protection Act 1998. Identify two specific requirements this guidance might include.

1 mark (max 2 marks) for any **two** of the following (**not** repeating a response already given on previous page):

- unauthorised devices do not access sensitive data / authorised devices only access data approved for BYOD / limit information shared by devices / limit access
- staff leave, device no longer used, all sensitive data removed / regular audits / staff agreement
- personally owned devices included in company MDM
- authentication - usernames and passwords not to be shared
- mobile devices lost or stolen, limit losses, learn from incident
- inspection - virus and malware clear
- CYOD rather than BYOD

2

17.6	**Multi-factor authentication provides greater security by requiring more than one identifier. Give two examples of possible access control combinations.** **1 mark** (max. 4 marks) for each example, eg • Something the user **knows** username, password, PIN • Something the user **has** smart card, dongle, safeword key, physical, hard token • Something the user **does** the way he/she speaks or types, sometimes called "behavioural biometrics" • Something the user **is** fingerprint, retinal, biometrics	**4**

Assessment outcomes coverage

Assessment Outcomes	Marks and % of marks available in section A	Marks and % of marks available in section B	Total Marks
AO1	12 marks 24%	22 marks 74%	34
AO2	14 marks 28%	4 marks 13%	18
AO3	12 marks 24%	0 marks 0%	12
AO4	12 marks 24%	4 marks 13%	16
Total marks	**50 marks**	**30 marks**	**80**

Question	Assessment Outcome 1	Assessment Outcome 2	Assessment Outcome 3	Total
1	1			
2		1		
3	1			
4		1		
5	1			
6	1			
7	2			
8	2			
9		2		
10	1, 3			
11		4		
12			6	
13				
14		2, 2, 2		
15			6	
16				
17	4, 8, 8, 2			
Total marks	**34**	**18**	**12**	**80**