Unit:
Network Security and Cryptography

Assignment title:
Smith and Jones Auctions

Sample Marking Scheme

Markers are advised that, unless a task specifies that an answer be provided in a particular form, then an answer that is correct (factually or in practical terms) **must** be given the available marks. If there is doubt as to the correctness of an answer, the relevant NCC Education materials should be the first authority.

This marking scheme has been prepared as a **guide only** to markers and there will frequently be many alternative responses which will provide a valid answer.

Each candidate's script must be fully annotated with the marker's comments (where applicable) and the marks allocated for each part of the tasks.

Task	Guide	Maximum Marks
1	***The term information assets have been limited to electronic assets, the most valuable of which will be data. This section is aimed at students identifying what is of real value in the company and the risks associated with it. Whilst a full risk assessment would consider threats and vulnerabilities separately, I decided not to complicate it here.*** ***Since ecommerce/e-auction is projected to be the main sales channel, risks to it should be considered as high.*** ***Highest value data will be business critical (contract, employee personal data, Customer data, Ecommerce/ e-auction site (auction data)).*** ***a) Marks: 2 for identifying appropriate assets*** ***b) Marks: 5 for identifying appropriate threats which should include accidental, system, malicious (Malware, Eavesdropping on transmitted data, hacking (external), Internal (e.g. weak access control, policies), equipment failure, DOS attacks. Availability issues are critical for the ecommerce and confidentiality particularly for finance and systems containing personal data (eg payments). Legal compliance issues and PCI DSS.*** ***c) Marks: 2 for making reasonable assessment of likelihood and impact.*** ***d) Marks: 1 for applying risk matrix correctly***	***2*** ***5*** ***2*** ***1*** ***10***
2	***a) Controlling the threats (2 marks per point with explanation) This will rather depend on the threats that they have identified:*** ***1) E-commerce related threats – must be included for full marks*** ***i) Availability is critical for ecommerce, so a cloud/ CSP solution with resilience is likely. Good answers will discuss DDOS mitigation, but a small company is unlikely to start with that and wait until the risk is deemed very high.*** ***ii) Eavesdropping or Spoofed web sites: TLS (can be awarded for part b)*** ***iii) Hacking*** ***(1) stored card data: for the company better to have 3rd party services such as WorldPay, SagePay or Paypal. This will transfer the risk. If an in-house system is justified, then risks are much higher – hashing/ encryption/ PCI DSS requirements are all in house. Reward any correct discussion of PCI DSS.***	***Up to 30***

Task	Guide	Maximum Marks
	(2) Website vulnerabilities – SQL injection/ XSS/ PHP/ non-default configuration, patching – pentest vulnerability analysis on regular basis is worthwhile 2) Internal: i) Acceptable use policies, contracts. InfoSec policy ii) Strong password (technical) policies. iii) Access controls on folders, iv) Restrictions on downloads. limit exchangeable media, Dropbox etc v) Monitoring. 3) System: i) Resilience – backup, redundant hardware, UPS etc. ii) Cloud services (eg Office365) for some information (depends on service level agreement/ trust as to what level of critical data are hosted in cloud) iii) Upgrading Win Server 2012 to 2016 or later 4) External: i) Malware: anti-malware ii) Secure configuration of systems to avoid defaults/ hardening iii) Encryption of sensitive data at rest and in transit (email/ File transfer) iv) Firewall / DMZ/ Proxy to control traffic v) Patch management vi) Split NAT 5) Vulnerability assessment b) Encryption 1) TLS for Ecommerce data in transit. 2) IPSEC for site to site 3) Symmetric encryption for critical data at rest (EFS) Critical Discussion of any alternatives	Up to 10 5 45
3	a) Setting up the VPN Award 4 mark for valid explanations listed below to max 12. 1) Essay explaining web-based or IPsec VPNs i) A good answer will Explain the terms intranet and extranet, differences and how they could be used in this example (4 points) ii) Recommendations for Ecommerce/auction servers best hosted by ISP or cloud to their branch sites. On premises solutions requiring additional security	12

Task	Guide	Maximum Marks
	and redundancy are acceptable detailed explanations. (4 points) ***iii) Good answers will show virtual secure connection for the auction with (TLS VPN solutions) or detailed explanation of IPSEC dependent on solution chosen (4 points)*** ***b) VPN Site to site*** ***i) Diagram including: Clearly labelled VPN endpoint for main site and all branch offices (firewall or Router with VPN features in correct locations) (4 marks)*** ***ii) Internal networks components in line with scenario and internet connections (2 marks)*** ***c) ACL and firewall explanation*** ***i) Give 4 points for Firewall explanation at the end of VPN's (including any or all UTM, DPI, IPS, NGFW features for ingress egress screening)*** ***ii) Give two marks for each ACL or other Firewall rule, point that relates a feature of the network solution to the risks in Task 1.*** ***iii) Give 2 marks for any valid extended ACL design.***	***6*** ***12*** ***30***
4	***Expect to see reference to:*** ***a) Training*** ***b) Policies – for staff and Customers*** ***c) Vulnerability assessment*** ***d) Other audit.*** ***e) Contracts and or user acceptance check box*** ***Up to 1 mark for explanation of each point***	***5***

5	**0-3**	**4-6**	**7-10**	
	Provides a brief description of the learning that occurred and a somewhat superficial analysis of its importance.	***Provides a description of the learning that occurred supported by some analysis which would benefit from more substance.***	***Provides an in-depth description of the learning that occurred and a developed analysis of its importance.***	
	Produces a simple action plan that gives limited or vague detail on the activities that need to take place in order to improve learning or practice.	***Produces a sensible action-orientated action plan that provides some detail on activities that need to take place in order to improve learning or practice.***	***Produces a comprehensive, action-orientated action plan that details clear activities that need to take place in order to improve learning or practice.***	
				10

Learning Outcomes matrix

Task	Learning Outcomes assessed	Marker can differentiate between varying levels of achievement
1	6,5	Yes
2	1,2,3,4,6	Yes
3	1,2,3,7,8,9	Yes
4	5,6	Yes
5	All	Yes

Grade descriptors

Learning Outcome	Pass	Merit	Distinction
Understand the most common types of cryptographic algorithm	Demonstrate adequate understanding of common types of cryptographic algorithm	Demonstrate robust understanding of common types of cryptographic algorithm	Demonstrate highly comprehensive understanding of common types of cryptographic algorithm
Understand the Public-key Infrastructure	Demonstrate adequate level of understanding	Demonstrate robust level of understanding	Demonstrate highly comprehensive level of understanding
Understand security protocols for protecting data on networks	Demonstrate adequate understanding of security protocols	Demonstrate robust understanding of security protocols	Demonstrate highly comprehensive understanding of security protocols
Be able to digitally sign emails and files	Demonstrate ability to perform the task	Demonstrate ability to perform the task consistently well	Demonstrate ability to perform the task to the highest standard
Understand Vulnerability Assessments and the weakness of using passwords for authentication	Demonstrate adequate level of understanding	Demonstrate robust level of understanding	Demonstrate highly comprehensive level of understanding
Be able to perform simple vulnerability assessments and password audits	Demonstrate ability to perform the task	Demonstrate ability to perform the task consistently well	Demonstrate ability to perform the task to the highest standard
Be able to configure simple firewall architectures	Demonstrate adequate level of understanding and ability	Demonstrate robust level of understanding and ability	Demonstrate highly comprehensive level of understanding and ability
Understand Virtual Private Networks	Demonstrate adequate level of understanding	Demonstrate robust level of understanding	Demonstrate highly comprehensive level of understanding
Be able to deploy wireless security	Demonstrate ability to perform the task	Demonstrate ability to perform the task consistently well	Demonstrate ability to perform the task to the highest standard