Unit:
Network Security and Cryptography

Assignment title:
Turing Hill Fire and Rescue Service

December 2015 – Sample Assignment

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.

Throughout the marking, please credit any valid alternative point.

Where markers award half marks in any part of a task, they should ensure that the total mark recorded for the task is rounded up to a whole mark.

Task	Guide	Maximum Marks
1	The term ‘information assets’ is limited to electronic assets and the most valuable asset is data. This section asks students to identify important network issues in an organisation and the risks associated with it. Highest value data will be business critical (contract, personal data, Intellectual property). **a)** Award 2 marks for identifying appropriate assets **b)** Award 5 marks 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 etc. **c)** Award 2 marks for making reasonable assessment of likelihood and impact. **d)** Award 1 mark for applying risk matrix correctly.	**10**
2	**a)** This task asks students to discuss threats and propose recommendations that would reduce risks. Recommendations can be separated into three areas: internal; system and external. Award up to 2 marks for each bullet point: <u>Internal</u> • Acceptable use policies, contracts. InfoSec policy • Strong password (technical) policies. • Access controls on folders, • Restrictions on downloads, exchangeable media, Dropbox etc • Monitoring. • Laptops encrypted (eg Bitlocker) • Mobiles have remote wipe • Sandbox to separate personal apps from company apps on iPad • Wi-Fi security – encryption/ authentication <u>System</u> • Resilience – backup, redundant hardware, UPS etc. • Redundant hardware, BCM policy and contract for disaster recovery. <u>External:</u> • Malware: anti-malware • Secure configuration of systems to avoid defaults/ hardening • Encryption of sensitive data at rest and in transit (email/ File transfer) • Firewall / DMZ/ Proxy to control traffic • VPN for external users • Site to site VPN for Data centre to Fire stations • Patch management • Vulnerability assessment	**30**

Task	Guide	Maximum Marks
	b) Encryption. A holistic approach should be taken to marking this sub-task. Key points can include: • VPN – site to site IPSEC can be shared key or certificate based for Fire stations to data centre. • VPN from mobile device – could be SSL or IPSec. AES for symmetric encryption • WiFi – WPA2- enterprise – RADIUS/ AES/ PEAP (could use PSK/ Hidden SSID/ MAC filtering etc) at Fire stations. • At rest – symmetric key encryption (EFS) **c)** Critical Discussion of any alternatives	**10** **5** **45**
3	The diagram should show connections to networking equipment such as firewalls, servers, PCs, routers at the command (data) centre. **a)** Award up to 3 marks for each bullet point: • Site to site VPN, Firewall at each site, • DMZ at head office including email server Tri homed or dual homed. • Proxy use is acceptable too if justified. • Internal network: Domain controller/ UPS / Backup system. • Clearly labelled routers/ switches. **b)** IP addressing • Private IPs and NAT (PAT) on internal network except DC. Static NAT ok in DMZ • Brief explanation of VPN / NAT expected **c)** Firewall rules should list source net/dest network/ protocol/ access/ for DMZ/ internal/ External/ VPN	**15** **10** **5** **30**
4	Award up to 5 marks for a good discussion. There should be reference to training, policies, audits and a vulnerability assessment.	**5**
5	A holistic approach should be taken to marking the reflective commentary. Award up to 10 marks for justified discussion on what learned and what would be done differently.	**10**
		Total: 100 Marks

Learning Outcomes matrix

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