These are the answers for 3D3 security.

My approach to marking is to make it relatively easy to get to 40-50, a bit harder to go to 60 and quite hard to get above 70. So in any marks-from-5 situatation, the 1st 2-3 are easily gotten, the next a little less and the last mark is hard to get.

4.

(a) Describe the concept of ”risk” as it applies to computer systems. (5)

Main thing here is that they don't go overboard and do recognise that all systems involve ”risk” - the actual words used to say that are less important.
*Marks from 4 for a basic good descrition, if they mention risk=vulnerabilty * impact or eqiuvalent then marks from 4; One more mark for excellent answers.*

(b) Describe two examples of network vulnerabilities and implmentation vulnerabiliies (5)

One mark each, plus one for interesting examples; Examples: network - a networked PS printer could be taken over and forward print jobs; network - cross site scripting of all sorts; imlementation - buffer overruns anywhere; implementation - insecure default settings

(c) Describe a countermesaure for each of the examples you chose in part (b) (5)

One mark each plus one for interesting examples; PS printer - firewall printers so they can't originate outbound connections; XSS - user training or IDS or firewall or browser updating discipline; buffer overruns - least privilege or code analysis or Java; insecure defaults - developer training

(d) What new vulnerabilities do you consider likely to become more important over the next few years (5)

Main point here is that the answer isn't crazy and isn't considered ”very important” today. For example - SOHO gateway zombies; virtual reality (e.g. 2nd life) or social network reputation kidnapping; Straight marks from 5, but strictly marked. (These are the bonus marks.)

5.

(a) Outline some of the common reasons for sending spam (5)

Marks from 5, need to include 2-3 reasons or more; one mark for each sensible justifed reason; examples - spread malware, stock pumping, advance fee fraud, sale of illicit goods (pharma), phishing;

(b) Describe how DKIM attempts to ameliorate the spam problem (10)

Marks from 7 for describing how DKIM works; marks from 3 for saying how that addresses spam;
How it works; about one mark each for: header signing, not-S/MIME or PGP, use of DNS, not a PKI, c14n and algorithm agility, SSP
Why it addresses spam: scales to Internet (cause no PKI, DNS etc); unsigned or badly signed same thing, allows building whitelist or foundation of reputation services;

(c) What will be the effect of widespread adoption of DKIM? (5)

This is the "advanced" bit, straight marks from 5 for sensible prediction. Possible points: DKIM makes it easier for bigger mail providers than for smaller ones; requirement to control your DNS increased; eventually, a lack of willingness to accept unsigned mail; spammers will get more interested in crypto - maybe try attack MTA more than before

6.

You are a system designer developing a new social-networking supported web-based mail application.

Important that they get the right requirements,design split in this question.

(a) Describe the main requirements you would try to meet, in order to protect your users from spam and other malware (10)

Marks from 2 for each of 4 requirements, then another 2 for overall goodness. Possible requirements:- false positive/negative managment (reduced rates, ability to feedback); leverage local users' reputation (e.g. only accept messages from "gold+" users); allow all-to-all messaging (don't impose unwaned limits); outbound controls (so that our users don't become sources of spam via botnet); choices for classification (e.g. only accept from pals, etc.); privacy protection (providing once-off/pseudononymous outbound addresses); use profiles to help detect spam (if profile says "female", be stricter with male oriented spams); be accountable for outbound mail (DKIM); prefer mail with accountable senders (DKIM)

(b) Briefly describe how you would meet each of those requirements (5)

Done above already. Hopefully DKIM as well.

(c) What would be the effect of the system design outlined above? (5)

They should argue why their design reduces inbound and/or outbound spam and why spammers won't target this set of users.

(d) Lastly, given all of the above, describe how you would attack the system, if you were a spammer (5)

Various. Straight marks from 5, with a bias towards inventiveness. E.g. re-transmission/replay of DKIM-signed messages;