Tutorial Sheet Week 4

Question 1

Why is it good practice to rebuild a firewall before it is installed?

Because there is no guarantee that it hasn't been hacked before installation.

Question 2

1. Why is it essential that an organisation develop a security programme?

   A security programme is a way for an organisation to manage risk. It ensures that those risks that most threaten an organisation are given the highest priority in terms of funding and effort and that when an event occurs, procedures for dealing with it are developed and known before it occurs.

2. A Denial of Service attack deals with which Security Policy issues?

   Communications and operations management

   Access control

3. You are to do a Risk Analysis for the online banking system of a large national bank. What is the risk associated with the following events? Which would you devote most effort and funding to prevent?

   (Note: Your answers may be quite different to the following. That is quite acceptable. What is important is that in answering this question you must justify your answer.)

   a. Phishing for customer accounts and PINs.

   Likelihood 4, Impact 2, Risk 8

   Despite customer education, some customers may be phished. The impact on the organisation is mostly reputational so must be dealt with. Phishing is unlikely to halt operations or threaten the bank's existence

   b. Transaction website hacked

   Likelihood 2, Impact 3, Risk 6

   As discussed in the tutorial, the context for this is that the website is already reasonably well protected so attacks are unlikely and the hacking consists of defacing. Given the bank's high profile and potential financial payoff should an exploit succeed, it is an attractive target so there. The impact would be reputational rather than operational.

   c. Transaction database hacked

   Likelihood 4, Impact 5, Risk 20

   Again, as discussed in the tutorial, the bank has very good database security but there has been some evidence that the database system we use is subject to a recently developed malware attack. Consequently, without action, there is a reasonably good risk of hacking occurring. The damage to the bank should it occur would be enormous, being reputational and operational.

   d. Denial of Service attack on transaction website

Tutorial Sheet Week 4

Likelihood 5, Impact 3, Risk 15

Given the bank's high profile, denial of service attacks are frequent. We have software in place to deal with it, but need to defend against novel attacks.

Our priorities will be:

1. Transaction database security (20),
2. Preventing DOS, (15)
3. Dealing with Phishing of customers (8)
4. Preventing Website hacking (6)

Tutorial Sheet Week 4

Question 3

1. Suppose we have a stateful packet filter firewall that validates the three-way handshake in a TCP connection

   a. What states will the firewall record for each step of the three-way handshake?

   New, New unreplied, Established

   b. Write packet filtering rules for each state.

State	SYN set	ACK set	Action	New state
New	Yes	Yes	Deny	
New	No	Yes	Deny	
New	No	No	Deny	
New	Yes	No	Allow	New unreplied
New unreplied	Yes	No	Deny	
New unreplied	No	Yes	Deny	
New unreplied	No	No	Deny	
New unreplied	Yes	Yes	Allow	Established
Established	Yes	No	Deny	
Established	No	No	Deny	
Established	Yes	Yes	Deny	
Established	No	Yes	Allow	Established